Ж У Р Н А Л   О Т   К О М П Ь Ю Т Е Р Н Ы Х   Х У Л И Г А Н О В

ХАКЕР

ver 08.02 (44)

W W W . X A K E P . R U



МАССИВНЫЙ IRC FLOOD

Используем Perl для IRC-атак

ЛУЧШИЕ МАМЫ НА СВЕТЕ

Самые крутые материнки под Pentium4

ИНТЕРНЕТ-2

ТЕХНОЛОГИЯ ИНОПЛАНЕТЯН



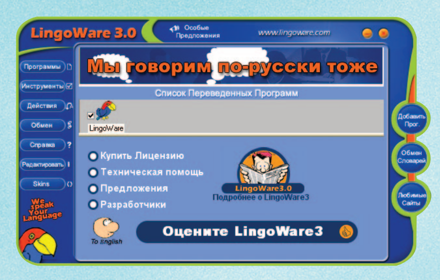
ПОДНЯТИЕ ЛОКАЛКИ В ЛИНУКСЕ С НУЛЯ

От азов до нюансов



ХОЧУ ЗНАТЬ ЮНИКС!

Где и как научиться Юниксу



РУССИФИКАЦИЯ СВОИМИ РУКАМИ

Как ковыряться в ресурсах и все там изменять



GTA3: РУКОВОДСТВО АНАРХИСТА

О чем не напишут в мануалах

SOFTWARE

ТОЛЬКО ДЛЯ ТЕХ, КТО ДЕРЖИТ В РУКАХ НОМЕР С ДИСКОМ

НА ДИСКЕ ТЕБЯ ЖДУТ 700МB СОФТА, ВКЛЮЧАЯ:

- СОФТ: Dreamweaver MX, PGPfreeware 7.0, Source Code Scaners, Agnitum Outpost Firewall, Panda Antivirus Titanium, Retina Apache Chunked Scanner 1.0.3, Tweak-XP 1.34.1, ACDSee 4.02, Win2000 SP2, Windows 2000 security patch
- ДРАЙВЕРА: Intel, SiS, Matrox, Creative, S3
- ЮНИКС: Весь софт из Юниксоида, все новые ядра, SNORT, BIND, Apache, Sendmail
- КОДИНГ: Компоненты для Delphi и C++ Builder, Исходники из "Кодинга"
- БОНУС: Программы с конкурса X, RU.LINUX FAQ

А также музыка и демки лучших команд

Philips Brilliance Line

мониторы высокого разрешения

BRILLIANCE®
HIGH RESOLUTION MONITORS

100% плоские,

еще более долговечные

Brilliance 201P10
- 21" (20" видимая область)
- Строчная частота 30 – 121 kHz
- AG Real Flat
- TCO 99

Brilliance 109P20
- 19" (18" видимая область)
- Строчная частота 30 – 111 kHz
- AG Real Flat
- TCO 99

Brilliance 107P20
- 17" (16" видимая область)
- Строчная частота 30 – 92 kHz
- AG Real Flat
- TCO 99

Товар сертифицирован

DEPO	(095) 969 21 11	Информатика	(8632) 99 01 01
Image.ru	(095) 737 37 27	МВидео	(095) 777 777 5
Ultra Computers	(095) 729 52 44	Параллакс	(8432) 93 55 46
USN Computers	(095) 775 82 02	Партия	(095) 787 70 07
А-Эл-Джи Софт	(4162) 35 2030	Систек	(095) 781 23 84
Белый Ветер	(095) 730 30 30	СтартМастер	(095) 784 63 83
Берёзка	(095) 362 78 40	Техносила	(095) 777 8 777
Европа	(3462) 515 555	Формоза	(095) 234 21 65

Срок гарантии – 3 года

www.ce.philips.ru



PHILIPS

Изменим жизнь к лучшему.

+БРАТСКАЯ МОГИЛА+

/РЕДАКЦИЯ

>Главный редактор
Сергей «SINtez» Покровский
(sintez@real.xakep.ru)
>Редактор ВЗЛОМ
Иван «Cutter» Петров
(cutter@real.xakep.ru)
>Редактор PC ZONE
Михаил «Centner» Михин
(centner@real.xakep.ru)
>Редактор JoyStick
Александр «2poisonS» Сидоровский
(2poisonS@real.xakep.ru)
>Редактор Ferrum
Константин «p0r0h» Буряков
(p0r0h@real.xakep.ru)
>Редактор UNIXOID
Артем «Cordex» Нагорский
(cordex@real.xakep.ru)
>Редактор CD
Николай «Avalance» Черепанов
(avalanche@real.xakep.ru)
>Корректор
Виталий Петрович
(vp@real.xakep.ru)

/ART

>Арт-директор
Петров Кирилл «KROt»
(kerel@real.xakep.ru)
>Дизайнеры
Алик Вайнер «Jmurik»
(alik@real.xakep.ru)
Евгений Чарский
Андрей Бондаренко

/PR

>PR менеджер
Губарь Яна
(yana@gameland.ru)

/INET

>WebBoss
Скворцова Алена
(Alyona@real.xakep.ru)
>Редактор сайта
Леонид Боголюбов
(xa@real.xakep.ru)

/РЕКЛАМА

>Руководитель отдела
Игорь Пискунов
(igor@gameland.ru)
>Помощник руководителя
Емельянцева Ольга
(olgaeml@gameland.ru)
>Менеджеры отдела
Алексей Анисимов
(anisimov@gameland.ru)
Басова Ольга
(olga@gameland.ru)
Крымова Виктория
(vika@gameland.ru)
Авдеев Владимир
(avdeev@gameland.ru)
Рубин Борис
(rubin@gameland.ru)

тел.: (095) 229.43.67
(095) 229.28.32
факс: (095) 924.96.94

/PUBLISHING

>Учредитель и издатель
ООО «Гейм Лэнд»
>Директор
Дмитрий Агарунов
(dmitri@gameland.ru)
>Финансовый директор
Борис Скворцов
(boris@gameland.ru)

/ОПТОВАЯ ПРОДАЖА

>Руководитель отдела
Владимир Смирнов
(vladimir@gameland.ru)
>Менеджеры отдела
Андрей Степанов
(andrey@gameland.ru)
Самвел Анташян
(samvel@gameland.ru)
тел.: (095) 292.39.08
(095) 292.54.63
факс: (095) 924.96.94

>Технический директор
Сергей Лянге
(serge@gameland.ru)

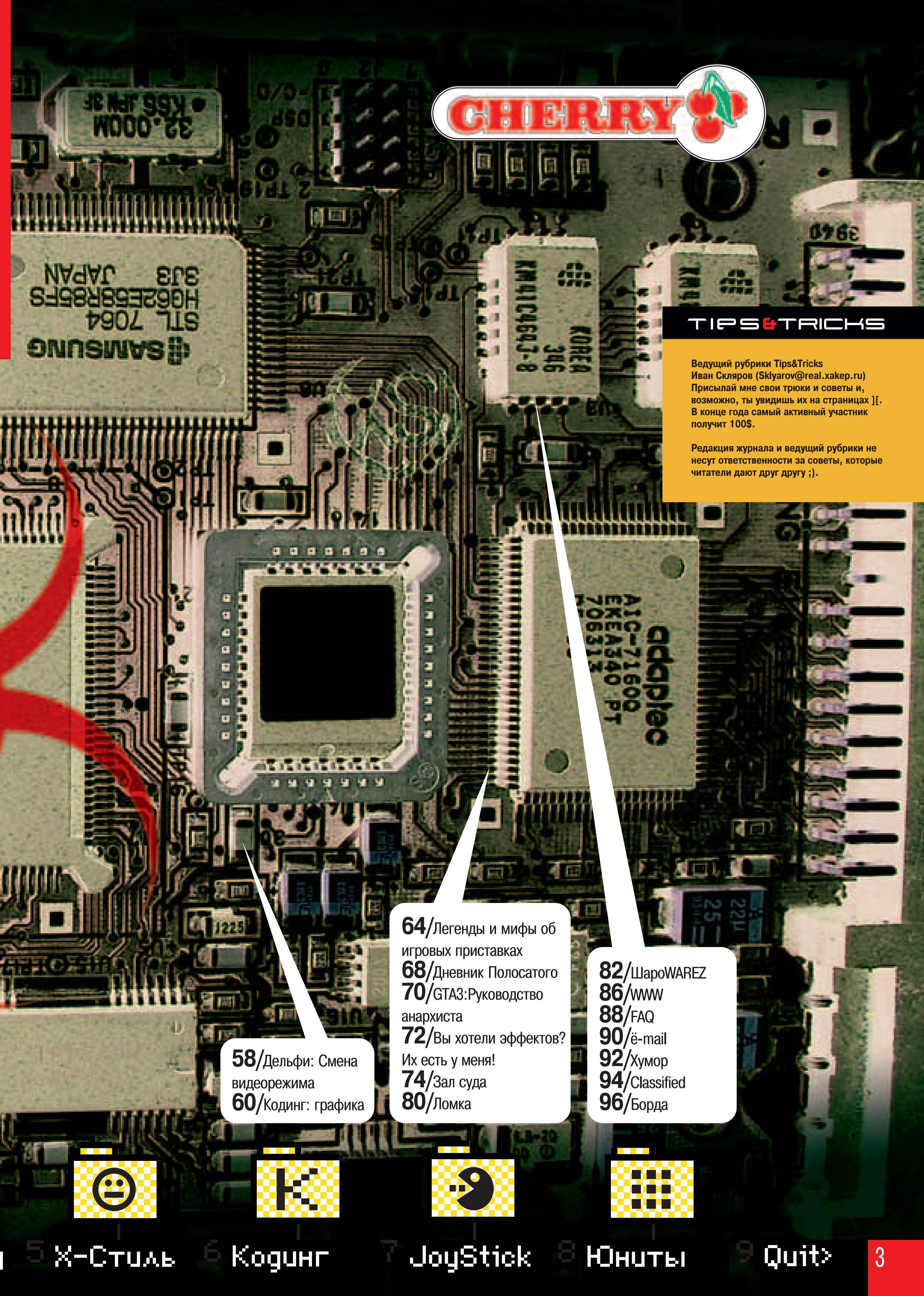
>Для писем
101000, Москва,
Главпочтамт, а/я 652, Хакер
http://www.xakep.ru
magazine@real.xakep.ru

Зарегистрировано
в Министерстве Российской Федерации
по делам печати, телерадиовещанию
и средствам массовых коммуникаций
ПИ № 77-11802
от 14 февраля 2002 г.

Отпечатано в типографии
«**ScanWeb**», Финляндия

Тираж **75 000** экземпляров.
Цена договорная.



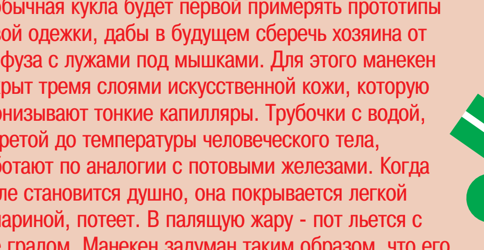


TIPS&TRICKS

Ведущий рубрики Tips&Tricks
Иван Скляров (Sklyarov@real.xakep.ru)
Присылай мне свои трюки и советы и, возможно, ты увидишь их на страницах][.
В конце года самый активный участник получит 100$.

Редакция журнала и ведущий рубрики не несут ответственности за советы, которые читатели дают друг другу ;).

!!! Алекс Целых (News@real.xakep.ru)



ПОТНЫЙ МАНЕКЕН

В Гонконге изобрели потеющий манекен. Эта необычная кукла будет первой примерять прототипы новой одежки, дабы в будущем сберечь хозяина от конфуза с лужами под мышками. Для этого манекен покрыт тремя слоями искусственной кожи, которую пронизывают тонкие капилляры. Трубочки с водой, нагретой до температуры человеческого тела, работают по аналогии с потовыми железами. Когда кукле становится душно, она покрывается легкой испариной, потеет. В палящую жару - пот льется с нее градом. Манекен задуман таким образом, что его "суставы" подвижны и позволяют принимать любую позу. Специальные сенсоры на синей кукле регистрируют температуру, давление и уровень влажности окружающей среды. В силу этого модельеры могут досконально выяснить, как поведет себя одежка на "взмыленном жеребце", что поможет кроить прогрессивные скафандры и спортивные штаны, а также приятные во всех отношениях наряды для бомонда.



КАЛЕЙДОСКОП НА СПИЦАХ

Устройство Hokey Spokes от компании Illumination Design Works позволит крутить немое кино на спицах твоего байка. С вращением колес миниатюрный компьютер зажигает LED-индикаторы на лопастях, которые уже на скорости 10 км/ч эффектно переливаются разными цветами. Каждое устройство воспроизводит отдельный фрагмент графического дизайна или текста. Изначально запрограммированы 20 шаблонов, которые можно редактировать, проигрывать последовательно или случайным образом. На колесе удается разместить до 6 Hokey Spokes одновременно. Чем больше, тем четче выглядит картинка на малых скоростях. Ночью езда с затейливой иллюминацией превращается в настоящее удовольствие для самого велосипедиста и прохожих. Конструкция устройства такова, что оно крепится практически на любой байк с диаметром колеса от 24 дюймов. Hokey Spokes выполнен в водонепроницаемом корпусе, работает от 3 АА батарей и продается по цене 25 долларов за штуку.

ЖЕЛЕЗНЫЙ БЕГЛЕЦ

Один из роботов-участников эксперимента Live Robots, о котором Х писал в марте, вырвался на свободу и геройски погиб под колесами автомобиля. Напомним, что автономные роботы помещены в закрытый павильон, на всем пространстве которого "хищники" преследуют своих "жертв". Когда представитель отряда "хищников", маленький, но гордый робот по кличе Гаак остался без присмотра всего на 15 минут, он проломил стену и направился прямо к центральному входу. Благополучно преодолев ступеньки, Гаак добрался до ближайшей автостоянки, где был превращен в лепешку машиной одного из зевак.

КОРПОРАЦИЯ МОНСТРОВ

В лабораториях Йельского университета ставят беспрецедентные опыты на электронных зверушках. Робопсу Megabyte II вскрыли нос и вживили счетчик Гейгера. А в районе спины присобачили новый микропроцессор, извратив тем самым заводскую программу. Собака-мутант держит нос на источники гамма-излучения. По адресу rtsp://milhouse.cat.nyu.edu/docidog1.rm можно наблюдать, как робопсина прокладывает путь в радиоактивную зону. Научный отчет о проделанной работе предваряет фраза: "Где-то рядом с тобой, в счастливых семьях и магазинах игрушек находится армия собак-роботов. Сейчас они запрограммированы дружелюбно: выпрашивают пластмассовую косточку и поскуливают национальные гимны. Однако они способны на большее и всего лишь ждут дальнейших указаний".



ЗУБНОЙ ПРИЕМНИК

Английские инженеры сконструировали зубной имплантант, который принимает сигналы радиостанций и мобильных телефонов. Маленькое чудо состоит из приемника и миниатюрного вибрирующего устройства. Вживление имплантанта в зуб осуществляется в ходе рядовой операции по капремонту больного дупла. Далее вибрации через кости черепа поступают на внутреннее ухо человека, где и преобразуются в звук. Слышимость отличная, словно ди-джей расположился в твоей драгоценной черепушке. Зубной имплантант может представлять интерес для футболистов на поле, внемлющих командам тренера, а также брокеров, получающих биржевые котировки в ресторане, разжевывая при этом резиновый бифштекс. Конечно, особо незаменим он будет на экзамене, когда "внутренний голос" подскажет ответы на вопросы злополучного билета.

ЯЩИК ПАНДОРЫ

Компания Westphal Electronic представила черный ящик - аппаратный генератор случайных чисел. В устройстве ZRANDOM производится оцифровка термического шума, на основе чего генерируется настоящий хаос - непрерывный поток из случайных битов, от 50 до 800 тысяч в секунду. В отличие от псевдослучайностей, выкинутых на пальцах, эти последовательности не основаны на алгоритмах и не имеют скрытых корреляций. Устройство аутентичности выдержало самые жесткие испытания, которые подтвердили отсутствие статистических зависимостей. Стоимость черного ящика составляет от 550 до 760 долларов, в зависимости от конфигурации.

ПИВНОЙ ОРГАНЧИК

Фугой Баха на органе из пивных бутылок отметила свой полувековой юбилей компания Peterson, всемирно известный брэнд музыкальных инструментов. На месте трубок расположилась разнокалиберная посуда из-под пенного Гиннеса. Природа звука такая же, как у классического органа: воздух проходит через узкое горлышко бутылки и резонирует от стенок. Для извлечения звуков более широкого диапазона бутылки наполнены минеральным маслом, которое не испаряется со временем. Орган из бутылок настроен по всем правилам жанра, а потому не фальшивит. Компания Peterson уже выпустила промо-диск с записью современных и классических мелодий, исполненных на пивном органе, включая марш из Звездных Войн. Изготовление копии инструмента по индивидуальному заказу займет около 2 месяцев.

СИБИРСКИЙ ЦИРЮЛЬНИК

Финская компания Plustech представила шагающую машину для корчевания деревьев. На своих шести ногах металлический богомол передвигается во всех направлениях, крутится на месте и перешагивает через препятствия. Он прекрасно чувствует себя на крутом склоне и берется за любую лесозаготовительную работу, ловко управляясь со свежеспиленными бревнами. Мозг чудища - интеллектуальная компьютерная система, которая контролирует высоту заноса ноги и прочие характеристики движения. Управление из кабинки оператора ведется при помощи джойстика. Стальные зубы богомола жадно вгрызаются в статные стволы деревьев. Чоп-чоп-чоп - только щепки летят.

МОБИЛА ДЛЯ ИХТИАНДРА

На китайский рынок выбросили мобильники со сменными панельками из рыбьей чешуи. Китайский рынок сотовых телефонов, перенасыщенный однообразными предложениями, сейчас переживает резкий всплеск интереса к эксклюзивным моделям. Так, нездоровым спросом пользуется Eastcom EG888, обтянутый кожей жемчужного гурами, по цене около 650 долларов.

НИЧЕГО НЕ СЛЫШУ

Японские ученые разработали строительные материалы, которые не пропускают излучение сотовых телефонов. Деревянные панели с частицами никелево-цинкового сплава незаменимы при отделке помещений, где "соловьиные трели" запрещены, например, в библиотеках и кинотеатрах. Кроме всего прочего, волшебные панели решают проблему с помехами, которые создают беспроводные компьютерные сети.

NEXT

МАГИЧЕСКИЙ АРТЕФАКТ

Компания Actuality Systems представила хай-тек версию хрустального шара для гаданий. В современном исполнении магический артефакт преобразился в трехмерное проецирующее устройство. Образцы молекул, сложные архитектурные ландшафты и прочие диковинные картины можно наблюдать, обходя чудо-шар со всех сторон. Пересчет декартовых координат в сферические осуществляется на Pentium IV при помощи цифрового сигнального процессора. Платформа способна отображать до 100 миллионов вокселей в секунду на шаре диаметром 25,4 см. Скорость вращения шара - 600 оборотов в минуту. Внешнее покрытие выполнено из ударопрочного стекла. По заверениям компании, в новом году будет достигнута большая частота вращения, а нынешняя стоимость устройства - 40 тысяч долларов - снизится, минимум, раза в полтора.

!!! Алекс Целых (News@real.xakep.ru)

F2-R2: ВНИМАНИЕ, СНИМАЮ!

Японская компания Takara представила робота-помощника F2-R2, названного по аналогии с народным любимцем из "Звездных войн". Робот высотой всего 16 сантиметров создан в рамках новой концепции развития робототехники: теперь не так важна внешность электронного существа и его сходство с человеком, как нацеленность робота на служение людям. F2-R2 принимает сигналы хозяев с сотового телефона, включая и выключая бытовые устройства по требованию при помощи инфракрасных сенсоров. На мордашке робота закреплена простенькая видеокамера для произведения цифровых снимков. Роботу можно дать, например, такое задание, как отыскать заблудшего кота. Фото удивленной мохнатой физиономии, выглядывающей из-под дальней кровати, F2-R2 по Интернету высылает хозяину. Цена робота новой формации - всего 200 долларов. Клиенты ADSL-служб получат экземпляр бесплатно.

АСФАЛЬТОВАЯ ЛЫЖНЯ

Американская компания ZAP снизила цену на электронный буксир для роллеров и скейтбордистов. Красный PowerSki из сверхпрочного алюминия представляет собой двуколку на колесах с поручнями, за которые нужно крепко держаться, - конструкция типа газонокосилки. На поручне расположен рычаг переключения скоростей, газ и тормоз. 12-вольтный двигатель позволяет разгоняться до 26 км/ч. Тележка виляет из стороны в сторону, создавая на горизонтальной поверхности впечатление скоростного горнолыжного спуска. Дальность перемещения на одном аккумуляторе - до 11 км. Стоимость в интернет-магазине - около 400 долларов.



КОМПЬЮТЕРНЫЙ ФЕЙЕРВЕРК

Команда из американских пиротехников и программистов готовит феерическое зрелище, которое "бабахнет" на следующий День Независимости. Постановка яркого спектакля под занавесом из облаков - непростая задача. Высший пилотаж - синхронизация во времени всех элементов огненного шоу. Слить воедино огонь и музыку, звуки выстрелов и сценическое действо призваны сложные компьютерные расчеты. Программа Visual Show Director 4D учитывает гравитацию и погодные условия для имитирования фейерверка на экране монитора. Когда с режиссурой будет покончено, программа сама составит смету расходов и, наконец, с высокой точностью будет управлять зарядами, отмахивая залпы строго-настрого по замысленному сценарию.

ИНТЕРАКТИВНОЕ TV

"МТУ-Интел" и Silicon Information Technologies продвигают гранд-проект широкополосного интерактивного телевещания в Интернете. Первой возможность "искупаться" в бурных потоках мультимедийной информации появится у пользователей "Точка.ру" с ADSL-доступом. Технологии SGI позволяют транслировать звук и видео в режимах индивидуальной и групповой передачи на сотни тысяч компьютеров и ТВ-приставок. От оборудования SGI сегодня зависит работа таких "китов" вещания, как CNN, British Telecom и NASA. Не за горами день, когда и у нас можно будет заказывать телевизионные программы, кромсать сценарии интерактивных фильмов и делать еще массу интересных вещей.



ШАРОГОН

Американский ученый сообразил хай-тек устройство для бескомпромиссного раскладывания бильярдных шаров по лузам. Stochastics включает в себя переносной компьютер в рюкзаке за спиной, тонированные очки и видеокамеру. С частотой 30 раз в секунду камера производит рекогносцировку местности, фиксируя положение на столе каждого шара. В результате компьютерных вычислений угол и траектория оптимального удара выводятся на очки, то есть фактически проецируются на стол. Остается один за другим наносить лихие удары по "прочерченной" линии. Пока что устройство общей стоимостью около 3 тысяч долларов позволяет себе капризничать: игнорирует затемненные участки стола и не берет в расчет положение белого шара после удара. Что, в общем, не умаляет его обучающих возможностей для новичков. Однако, по уверениям разработчика, менее чем через 5 лет Stochastics легко обставит лучшего из шарогонов homo sapiens.

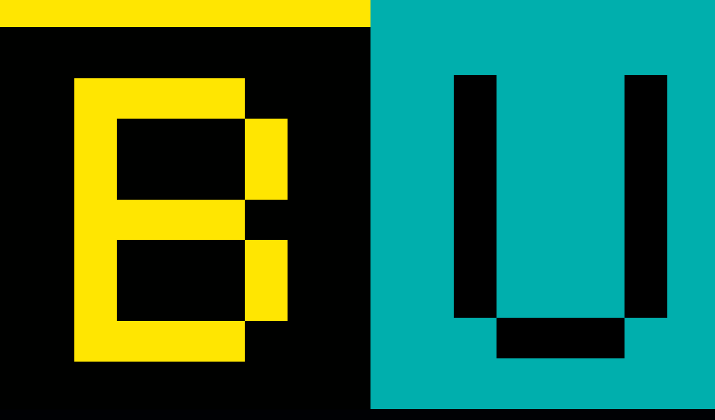
ХАЙ-ТЕК РАКЕТКА

Некоторые теннисисты, пасущиеся в первой десятке на престижном турнире French Open, играли "комфортными" хай-тек ракетками. Их выпуск освоила компания Head Sport AG. Сглаживание неприятных вибраций, как последствий удара по мячу, производится благодаря использованию струн из пьезоэлектрика. При прогибании струн в месте приема мяча на ракетку вырабатывается электрический разряд напряжением 600-800 вольт и силой в добрую сотню микроампер. Разряд поступает на компьютерный чип, размещенный в ручке ракетки, где производятся необходимые манипуляции с напряжением. В ходе обратного процесса, который начинается через 2-3 миллисекунды, разряд снова выдается на пьезоэлектрик, и ракетка разгибается в сторону удара, гася колебания. Правилами Международной федерации тенниса запрещено использование в ракетках батарей, поэтому схема на основе пьезоматериалов отвечает букве спортивного закона. Ракетки серии Head i.S18 Intelligence, представленной на рынок в чрезвычайно ограниченном количестве, продаются по цене 500 долларов.

СОЛОВЕЙ-РАЗБОЙНИК

Поражающим фактором нового типа вооружения, разрабатываемого Пентагоном, является звук. Не простой, а самый страшный и пугающий на свете - плач ребенка. Гиперзвуковая акустическая система будет прокручивать детский плач задом наперед на громкости от 140 децибел, сравнимой с ревом реактивного аэробуса. По расчетам американских военачальников, устрашающий сигнал на грани ультразвука вызовет настоящую панику в рядах противника, сопровождаемую невыносимыми головными болями. Бойцам, прошедшим родительскую школу, опасаться нечего.

!!! SideX (sidex@real.xakep.ru)
выпуск посвящается мл. лейтенанту А.Чичериной



■ Проблемы с файл-дескрипторами ядра Linux
■ BT id 5178
■ Класс - ошибка дизайна
■ Тип эксплойтинга - локальный
■ Дата - 19.06.2002
■ Уязвимый продукт - Multi vendor
■ Автор - Paul Starzetz paul@starzetz.de

Редко в разделе «Linux» BT Security Focus'а можно отыскать новые записи по конкретному дистрибутиву - проблем сколько угодно, а вот загвоздки «ядерного» уровня случаются не столь часто. Нечто похожее творится и с BSD-клонами, чей первенец - FreeBSD - оброс, сравнительно недавно, проблемами с файл-дескрипторами. В ту же Ахиллесову пяту было поражено ядро Linux.
Поражение, следует признать, неожиданное, т.к. еще в исследовании по FreeBSD основные Linux-дистрибутивы были протестированы на оригинальный free-шный баг. Обнаружено не было. Забыли лишь кусочка кода в fs/file_table.c, который ответственен за дополнительные слоты файл-дескрипторов, используемые root'ом. Боссам принято выделять специальные привилегии, как водится. Только вот не совсем боссовские setuid-бинарики a la «passwd» или «su» также способны подавить имеющиеся root-слоты. Избегая оригинального кода ядра, предлагаю просмотреть реакцию бажной системы на работу эксплойта, предложенного автором:

```
sidex@xakep:-> id
uid=500 (sidex) gid=100 (users)
sidex@xakep:-> ./fddos
errno 24 pid 24087 got 1021 files
errno 24 pid 24088 got 1021 files
errno 24 pid 24089 got 1021 files
errno 24 pid 24090 got 1021 files
errno 24 pid 24091 got 1021 files
errno 24 pid 24092 got 1021 files
errno 24 pid 24093 got 1021 files
errno 23 pid 24094 got 807 files
```

Нехитрой операцией достигается указанный лимит, поедая некоторые файл-дескрипторы (fd) root'a. Далее начинаем освобождение отдельных fd:

```
pid 24094 closing 809
 pid 24094 closing 808
 pid 24094 closing 807
 pid 24094 closing 806
 pid 24094 closing 805
 pid 24094 closing 804
 pid 24094 closing 803
 pid 24094 closing 802
Исполнение /usr/bin/passwd
Old Password:
```

Стартуем бинарик fddos'a (эксплойт) под обычным, неroot'овым пользователем на первом терминале:

```
xakep:~ #id
bash: /usr/bin/id: Too many open files in system
xakep:~ # w
bash: /usr/bin/w: Too many open files in system
```

Система убита!
Универсального, временного решения нет. Разве что установка глобального, для каждого юзера файлового лимита. Сие реализуется в контексте uid/euid-политики. Полный захват системы пока не был осуществлен по указанной уязвимости, но выглядит вполне возможным.

■ Переполнение буфера процедуры шифрования пароля в MS SQL 2000 Server
■ BT 5204
■ Класс - ошибка пересечения смежных условий
■ Тип эксплойтинга - удаленный
■ Дата - 10.07.2002
■ Уязвимый продукт - MS SQL Server 2000 (включая SP2)
■ Автор - MS Technet

Добрая половина июльского BT была поглощена проблемой SQL-серванта, что ветвисто развивалась из оригинального сообщения за номером 4847. Сегодня достигнутого объема дырок повторить не удастся, будет лишь парочка. Очевидно, искатели-колупатели MS'а ушли на летние каникулы - никаких новостей и про IE. Хотя скоро осень, 1 сентября, искатели вернутся из пионерских лагерей, и тогда только держись :).
Как часто бывает с переполнениями, рассматриваемая дыра обозначилась из отсутствия контроля над буфером процедуры шифрования пароля. Дополню, что подобная процедура юзается администраторами для идентификации подключающихся к информационному массиву SQL-сервера. Эксплойтинг осуществляется путем направления чрезвычайного объема данных как аргумента процедуры шифрования пароля. Итог - захват доступа к базе SQL, а также возможность исполнения процессов в системе с правами прохудившегося сервера (system, как водится). Эксплойта обнаружено не было.
Вторая проблема толком не ясна, т.к. на рабочей станции ее самому нащупать не удалось. SecFoc предательски молчит, а MS Technet (02-34 выпуск) отмазывается стандартным: заплатки пришивайте, а нос не суйте. Общие слова - получение контроля над SQL-сервером (целой системой) путем переполнения буфера процедуры контроля над заполнения таблиц SQL-сервера.
Третья проблема более визуальна. Поднятие уровня привилегий, как последствие некорректно обозначенного уровня доступа ключом реестра, содержащим информацию по учетной записи сервиса SQL Server'a. Немного послонявив реестр RegEdit'ом, злодей мог поднять свой доступ до системного уровня.
Собирательный патч по всем трем проблемам доступен в MS Update'e.
Рекомендации по безопасности типичны классическим выкладкам виктимологии. Минимум прав непроверенным пользователям - чуткое внимание группе администраторов, исключительная выдача xp_regwrite разрешения, ограничение доступа к процедурам «Окружением» (сделано по умолчанию). В подобных выкладках камуфлируется рекламный ход: не лезь - убьет, используешь «По умолчанию», как MS завещал, - все о'кэй. Неплохая тактика, успешно использованная координаторами OpenBSD дистрибутива.





■ Слежка за чужими процессами ktrace'ом в *BSD
■ BT id 5133
■ Класс - ошибка дизайна
■ Тип эксплойтинга - локальный
■ Дата - 27.06.02
■ Уязвимый продукт - FreeBSD (вплоть до 4.6), OpenBSD (вплоть до 3.1)
■ Автор - OpenBSD Security Team

Когда FreeBSD сдавала информацию по всем процессам системы, несмотря на ограничение юзера просмотром его собственных, OpenBSD держалась кремнем. Сейчас же обе системы оказались слабы перед утилитой ktrace, что занимается слежением за оригинальными и дочерними процессами системы. По задумке, по умолчанию только root может видеть все происходящее разом. В реальности же мы можем получить ряд конфиденциальных данных, вроде ссылок на файлы паролей и авторизаций, проскакивающих среди инфы о процессах в ktrace. Патчи готовы, хотя Free/Open security-спецы видят решение и в полном отключении Ktrace (работает в обеих системах по умолчанию) с перекомпиляцией ядра. Заплаточные изменения, в случае опробованной Фрюхи, коснулись файла src/sys/kern/kern_ktrace.c. Последнее: OpenBSD SecTeam - вовсе не очередная подростковая security-шайка, над которой смеяться уже моветон. OpenBSD SecTeam - официальный орган OpenBSD.

■ Звуковые схемы ICQ
■ BT id 5239
■ Класс - ошибка верификации доступа
■ Тип эксплойтинга - удаленный
■ Дата - 15.07.02
■ Уязвимый продукт - Mirabilis ICQ 2002 a build #3727
■ Автор - «xLaNT» xLaNT@mailfloor.ch

Файлы модулей расширения уже подводили ICQ не раз, вспомним лишь апрельский .hpf-конфуз. Сейчас проблемы творят файлы .scm - звуковые схемы. Оригинальное применение вполне понятно: можно менять набор звуков, которыми радует слух Аська.
Ты без проблем сможешь поменять «куку» на нечто нецензурное и смачное: достаточно лишь включить тэг на новую схему в IFRAME HTML-кода. К постингу BT прилагается пример - пустая схема, которая напрочь лишает ICQ всяческого звучания. Лично я последствий так и не заметил, последние 2 года работаю с рассматриваемым сетевым пейджером без звука (чего и тебе желаю). Искатель бага говорит о возможности обвала Аськи, а возможно и всей системы путем введения в .scm файл определенной последовательности ASCII-символов. Лично у меня ничего не вышло, даже после записи в файло всего греческого и узбекского алфавита :(. Впоследствии идея была доработана, и уже голландский исследователь предложил готовое решение, что позволит использовать текущий баг ICQ совместно с IE'шным для исполнения зловредного exe в системе. Линкуемся сюда http://www.xs4all.nl/~jkuperus/icq/icq.htm. Браузер, увидев ссылку на .scm, быстренько сливает схемку и извлекает указанный wav-файл. На первый взгляд безобидный звуковой файл в действительности оказывается .mht (файл почтового архива), который уже IE исполняет, руководствуясь собственной дыркой. А где выполненный .exe, там и гуляй поле… Официального решения пока не пришло. В перспективе Mirabilis'у следует научить Аську работать со звуковыми файлами из временных папок, чтобы злоумышленник не мог предугадать приблизительное расположение файла для дальнейшего exe-исполнения. Пока же заходим в «Панель управления»->»Опции папок»->»Типы файлов»->»SCM», прицепляем галку на «Запрашивать разрешения после скачивания».

!!! p0r0h (p0r0h@real.xakep.ru)

В номере:

АВГУСТ 2002
№44





Новенький Rio

Компания SONICblue родила на белый свет очередной плейер. Имя новорожденного - Rio 900. И хотя он как две капли воды похож на своего братца (Rio 800), по характеристикам он его превосходит. Так, например, объ-



ем памяти увеличился до 192 МБ (можно приобрести и дополнительные модули памяти на 32, 64 или 128 МБ), а работы NiMH-аккумулятора теперь хватит на 10 часов. Любимые форматы - MP3, WMA и Audible, но в будущем этот список может легко расшириться. Воссоединение с ПК происходит с помощью USB 1.1, а с магнитолой - через специальный кассетный адаптер. Покупка же такого девайсика обойдется ориентировочно в 250 американских енотов.

Bluetooth-адаптер от EpoX

Материнок от Epox с поддержкой Bluetooth пока в продаже не наблюдается, но зато уже имеется Bluetooth-адаптер Bluetooth Dongle BT-DG02 с USB-интерфейсом. Так что теперь можно подключать разнообразную периферию к мамкам, оснащенными соответствующими Bluetooth-модуля-



ми (например, EpoX BT-MD01 с внешней антенной). Ну а стоит этот адаптер около 50 бакинских.

nForce2 в массы!

NVIDIA с недавних пор нацелилась и на рынок системных чипсетов. Сначала был nForce, а вот теперь и nForce2. Чип будет выпускаться в двух вариантах - со встроенным графическим ядром (SPP) и без него (IGP). Вот краткие характеристики новинки:

Поддержка платформы на Socket A;
Два канала DDR400/DDR333/DDR266 (PC3200/PC2700/PC2100);
Встроенное графическое ядро класса GeForce4 MX;
AGP 8x;
ATA133;
USB 2.0;
Два контроллера 10/100 Ethernet MAC;
IEEE 1394;
Декодер Dolby Digital;
ACR.

Также, к радости АМДешников, ожидается, что сам чипсет, а соответственно и материнки на нем, не будут столь дорогим, как первый собрат.

Резак от Asus

Имя нового внутреннего CD-RW привода - Archont. Интерфейс - ATAPI. Скоростная формула, как всегда, впечатляет - 48x/16x/48x. Размер буфера, правда, стандартен - всего



2 МБ, но если учесть использование технологии защиты от переполнения FlextraLink и оптимизации скорости записи FlextraSpeed, то можно не беспокоиться за жизнь болванок. Записывать же болванки можно с помощью прилагаемого ПО - популярным Nero 5.5.

LOOX - это судьба!

Точнее не судьба, а название нового КПК от Fujitsu-Siemens. Начинка этой новинки достаточна продвинутая и привлекательная: процессор Intel PXA250 XScale на 400МГц, цветной TFT-дисплей с поддержкой до 65536 цветов и разрешением 240x320, объем памяти - 32Мб ROM и 64Мб RAM, инфракрасный порт, USB-порт, RS232, Bluetooth-модуль и разъем для подключения внешнего GSM/GPRS-блока. Также имеются слоты расширения для карт SD, MMC



и Compact Flash (тип II). Стоит же этот красавец немало - порядка 680-700 буказоидов.

Старым мамкам посвящается...

Компания PowerLeap выпустила два оригинальных комплекта для установки новых камушков 1,4ГГц Intel Celeron на материнки со Slot-1 и Socket 370. Называются они, соответственно, PL-iP3 и PL-370/T. Стоят - 170 вечнозеленых. Дороговато немного, но юзерам, искренне любя-



щим свою стареющую мамашу и заботящимся о ней, этот наборчик придется весьма кстати ;].

Резиновая Зина

Назвать ее Клавой язык не поворачивается, т.к. подобных экземпляров пока еще не было замечено в мире компов и периферии. Дело в том, что это первая растягивающаяся клавиатура.



Предназначена она в первую очередь для карманных ПК. Тесная связь происходит по Bluetooth, IEEE 802.11b или ИК порту. Материал, из которого сделана новинка, выполнен из некой эластичной и прочной резины, что позволяет ей растягиваться на два размера. А с таким размером уже можно печатать двумя руками, что, безусловно, понравится владельцам КПК.

Комедия от Olympus

И правда, цена на новую 4-мегапиксельную камеру от Olympus смешная. Всего-то 500 баксов :]. Имя цифровушки - CAMEDIA C-4000 ZOOM. Взглянем на ее характеристики:
Сенсор: 1/1,8», CCD, 4,1 млн. элементов, эффективное число пикселов - 4,0 млн;

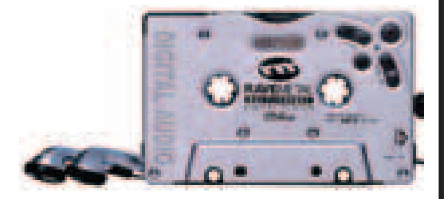


Цифровой зум: 3,3x;
Объектив: 3x оптический зум;
Фокусное расстояние: 6,5-19,5 мм;
Апертура: F:2,8;
Флэш-карта на 16МБ;
USB-интерфейс, Video-out;
2 аккумулятора.

Помниться, раньше аналогичная модель стоила целых 1100 бакинских...

Кассетный плейер MP3

Наверняка ты уже слушал или видел этот любопытный девайсик. Так вот, его производитель, Seagrand, выпустил новую версию - RAVEMETAL RM200M-256MB. Новинка имеет все тот же дизайн и практически те же



размеры и вес (100,4 х 63,8 х 12 мм, 55 граммов), поддержку MP3 и WMA, возможность подачи питания от «прикуривателя» автомобиля. Изменился лишь объем памяти (256МБ), да возросла цена. Однако и с незначительными изменениями такой плейер остается привлекательной покупкой.

7.1 звуковуха от Hercules

Небезызвестная Hercules планирует в скором времени представить свою звуковую карточку для построения многоканальной акустики (вплоть до 7.1) - Gamesurround Fortissimo III 7.1. Основные же спецификации будут иметь следующий вид:

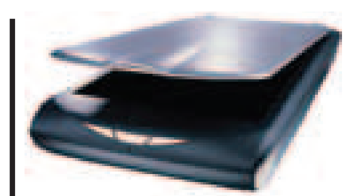
Шина PCI 2.14;
DSP процессор Cirrus Logic SoundFusion CS4624;
20-битный четырехканальный выход и 18-битный стерео выход, сэмплирование - до 48КГц;
Поддержка технологий: Sensaura 3D, Microsoft DirectSound 3D, EAX 1.0, EAX 2.0, A3D 1.0, I3DL2, MacroFX, MultiDrive, ZoomFX, EnvironmentFX, Microsoft DirectSound, DirectMusic, Dolby Surround, Dolby Digital;
Поддержка Dolby Digital EX 7.1 (для DVD);
Выход на фронтальные колонки, тыловые, центральную/LFE, седьмой и восьмой каналы, выход на наушники, Line in / Mic in, порт MIDI / Game (MPU 401), оптический S/PDIF выход.

Также вместе с этой звуковухой будут поставляться выносная панель Gamesurround Fortissimo III 7.1 addtive MIDI/Game, ПО и документация. Ориентировочное появление на прилавках - середина августа. Ждем-с...

Цветок от UMAX

Компания UMAX взрастила на своих плантациях новое детище - планшетный сканер UMAX Astra 6700 с интерфейсом USB2.0. Характеристики цветка:

USB 2.0/1.1 интерфейс;
Разрешение: 2400 х 4800dpi;
Сдвоенная CCD-матрица;
Разрядность (внутренняя и внешняя): 48 бит;
Габариты: 272 х 478 х 87 мм;
Вес: 2,8 кг.



ПО достаточно богатое и удобное: TWAIN-драйвер, утилита программирования «быстрых кнопок», OCR Abbyy Fine-Reader Sprint, редактор MGI PhotoSuite III SE, PaperCom Document Manager. Также к сканеру можно докупить слайд-адаптер TPU-6700 с полем 101 х 127 мм и рамками для пленок и слайдов. Цена же на Астру будет приличной - целых 250 вечнозеленых.

Охлаждающий вулкан

Уважаемая оверклокерами всего мира компания ThermalTake, представила свой новый медный кулер - Volcano 9. Охлаждать он должен горячие камушки от AMD и, судя по всему, делает он это довольно успешно. Эта оверклокерская игрушка имеет множество скоростных режимов (от 1300 до 5143 оборотов в минуту) и при этом спокойно справляется со своей обязанностью даже на



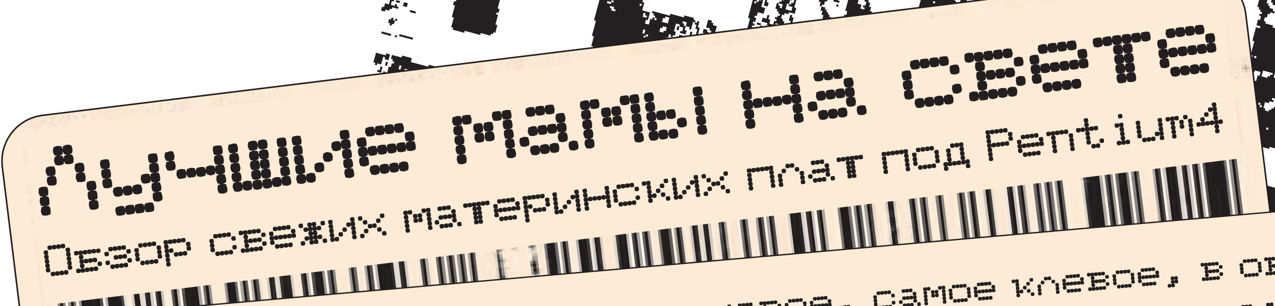
самых низких оборотах. Правда, стоить девятый вулканчик будет соответствующе - порядка 40-50 зеленоголовых.

Big Bang от HP



25 июля в нашей галактике, а точнее в славном местечке Нахабино произошел Big Bang. Жертв и разрушений, правда, не наблюдалось, но впечатлений от новых девайсов и технологий HP было масса. Особенно впечатлила новая линейка струйных принтеров (HP PhotoSmart 130/7150/7350 и HP DeskJet 3420/3820/5550), которая призвана заметить старых бойцов печатного фронта. Новички же рвутся в бой и стремятся показать свои самые лучшие качества: поддержку самых высоких разрешений (до 4800x1200), 6-ти цветную печать, скорость (до 17 стр/мин в черном цвете и до 13 стр/мин в цветном), а также фирменную технологию Photoret IV. Армия девайсов от HP, конечно, принтерами не ограничилась и призвала еще под свои знамена новые модели сканеров для дома, офиса и профессионалов (HP ScanJet 3570c/3530c/3500c/2300c, HP ScanJet 5550c/5500c/4570c/4500c и HP ScanJet 7400c/7450c/7490c) вместе с цифровыми камерами (HP PhotoSmart 320/620/720). Да, такая армия может легко облегчить жизнь многих юзверей, наполнив ее практичностью и удобст вом.

p0r0h (p0r0h@real.xakep.ru)



Лучшие мамы на свете

Обзор свежих материнских плат под Pentium4

Самая крутизна, самое новое, самое клевое, в общем – сегодня все самое-самое. Мы подобрали несколько топовых моделей материнок, которые только что появились на рынке и с нетерпением представляем их на твой суд. Читай, вникай, делай выводы.

MSI 845E Max2-BLR

Не материнка, а просто красавица. Причем как внешне, так и внутренне. Да и коробка оформлена словно для подарка. Стильное оформление сочетается с блестящим ламинированным покрытием. Такой грамотный подход к дизайну уже вызывает желание купить эту красавицу, даже не заглядывая внутрь коробки и не изучая спецификаций. Впрочем, все же нужно заглянуть под одежку и посмотреть, как обстоит дело там :].

Комплектация

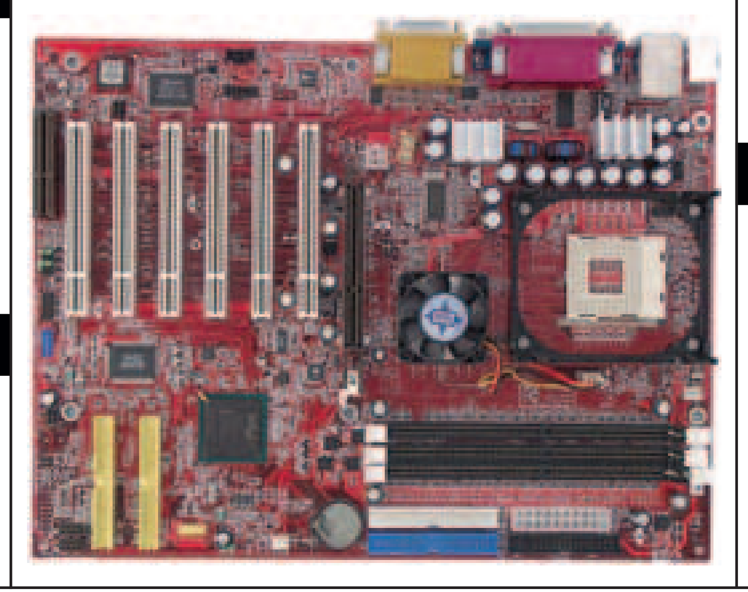
Внутри коробки дожидаются своего часа богатая документация, два кабеля ATA66/100/133, шлейф для подключения дисковода, три планки (USB-Bracket, S-Bracket и D-Bracket-2), дискета с драйверами для IDE RAID, комплект Bluetooth PC2PC и компакт с разнообразными драйверами и софтом для мониторинга и разгона системы.

Характеристики

Материнка основана на новом чипсете i845E от Intel и имеет поддержку 533 МГц шины. Основные же характеристики выглядят так: три разъема под память DDR, слоты расширения - AGP/ 6 PCI / CNR, порты ввода/вывода - 2 COM/ LPT/ 2 PS/2/6 USB 2.0. Также на плату интегрированы: звуковой контроллер на базе AC'97-кодека Avance Logic ALC650 с поддержкой аудиосистем 5.1, разъемом SPDIF и выходом для подключения фронтальных колонок; сетевой контроллер и IDE RAID, выполненный на базе микросхемы Promise PDC20276. Особого же внимания заслуживает комплект Bluetooth PC2PC, позволяющий устанавливать беспроводное соединение с сотовым телефоном, PDA, ноутбуком, другим компом и т.д. Например, для того, чтобы установить беспроводную связь между двумя компами, нужно вставить в имеющийся разъем карту расширения с одним из модулей Bluetooth с внешней антенной, а другой адаптер установить в USB-порт второго компьютера. Такой связи должно хватить на расстоянии до 200 метров, при этом скорость будет на уровне 700-723 Кбит/с. Только нужно учесть, что при работе модуля Bluetooth блокируется один из USB-портов (на USB-Bracket), поэтому лучше оставлять его всегда свободным. Благо других USB-портов предостаточно. Как видишь, характеристики платы не только впечатляют, но и могут служить ориентиром для других производителей.

Настройка и разгон

Отдавая дань моде, MSI 845E Max2-BLR имеет всего только одну перемычку для очистки CMOS, остальные настройки доступны только через BIOS. Правда, настроек там предостаточно: выбор таймингов памяти, выбор частоты работы памяти, ручное распределение прерываний по слотам, изменение частоты FSB (от 100 до 233 МГц с шагом 1 МГц), изменение коэффициента умножения процессора, изменение напряжения ядра процессора (от 1,5 до 1,85 В с шагом 0,025 В), памяти (2,5, 2,6, 2,7 и 2,8 В) и шины AGP (1,5, 1,6, 1,7 и 1,8 В). В общем, все, что нужно для тонкой настройки и оверклокинга.



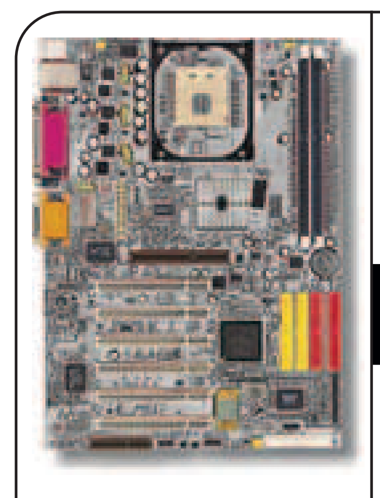


Soltek SL-85DR2+-L

Еще одна симпатяга, только на этот раз от Soltek. Коробка, правда, не такая стильная, как у MSI, но зато текстолит платы, оформленный под серебро, впечатляет. Сразу видно, что инженеры и разработчики отнеслись к этой мамаше со всей любовью, на которую только были способны :].

Комплектация

Помимо самой платы в коробке можно найти доки и руководство по настройке, два кабеля ATA66/100/133, шлейф для дисковода, дискетку с драйверами для IDE RAID, два компакта с драйверами и софтом для системы (в том числе и с PC-cilin 2002, Virtual Drive, PartitionMagic 6.0 SE, Drive Image 4.0 и т.д.), а также дополнительную планку с двумя USB 2.0 разъемами.



Характеристики

Сердцем этой мамаши является интеловский чипсет i845E с поддержкой 533 Мгц шины. К услугам же юзверя доступны два DDR слота, AGP, 6 PCI, CNR, порты ввода/вывода - 2 COM/ LPT/ 2 PS/2/4 USB 2.0. Имеется и звуковой контроллер на базе AC'97-кодека с поддержкой 5.1 акустики плюс сетевой контроллер и IDE RAID на базе чипа Promise PDC20276.

Настройка и разгон

Для того чтобы настроить плату на максимальную производительность, можно воспользоваться фирменной технологией Red Storm Overclocking, имеющимися перемычками для изменения напряжения на AGP (от 1.5 до 1.7 В) и на DIMM (от 2.5 до 2.7 В), а также воспользоваться разнообразными настройками BIOS. В общем, есть, где развернуться и показать все, на что способен ты и твоя система.

ASUS P4B533-E



И вот на подиум выходит многократная лауреатка всевозможных конкурсов - пафосная и великолепная ASUS ;]. Ей есть, чем похвастаться и что продемонстрировать. Итак, приступим к осмотру.

Комплектация

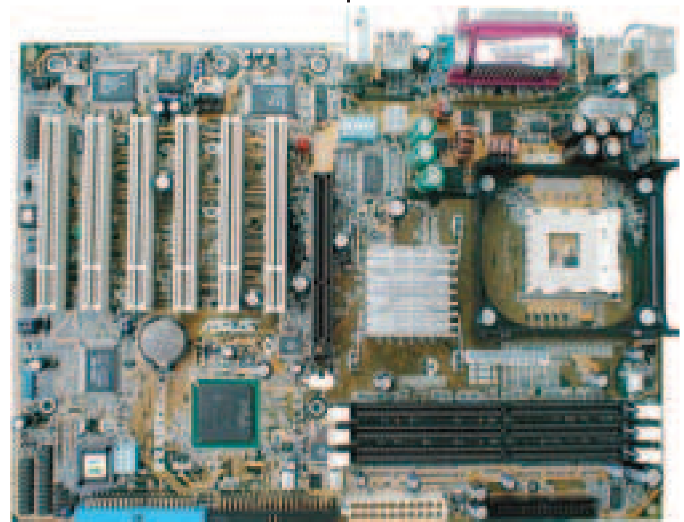
На самой коробке гордо демонстрируются надписи, возвещающие о поддержке самых передовых технологий и фишек. Например, о поддержке 533 МГц системной шины, ATA133 RAID, IEEE 1394, USB 2.0, БИОСе на разных языках и возможностью сделать свое лого при загрузке. В самой же упаковке тоже есть, чем поживиться: доки и руководства по настройке и установке, два кабеля ATA66/100/133 и один ATA33, шлейф для дисковода, диск с драйверами и софтом, дополнительная планка с двумя USB 2.0 разъемами, пакетик с перемычками, а также оригинальная наклейка для оверклокеров с описанием настроек платы и расположением соответствующих джамперов. Сразу видно, что разработчики не стали экономить даже на мелочах.

Характеристики

Естественно, характеристики на самом высоком уровне, и каких-либо упущений и недоработок не наблюдается: чипсет i845E, три разъема под DDR, слоты расширения - AGP/ 6 PCI / CNR, порты ввода/вывода - 2 COM/ LPT/ 2 PS/2/6 USB 2.0. Звуковой контроллер для подключения шестиканальной акустики (AC'97 2.2), контроллер для RAID (Promise PDC20276) и IEEE 1394 тоже на месте и только ждут подсоединения родственных девайсов :].

Настройка и разгон

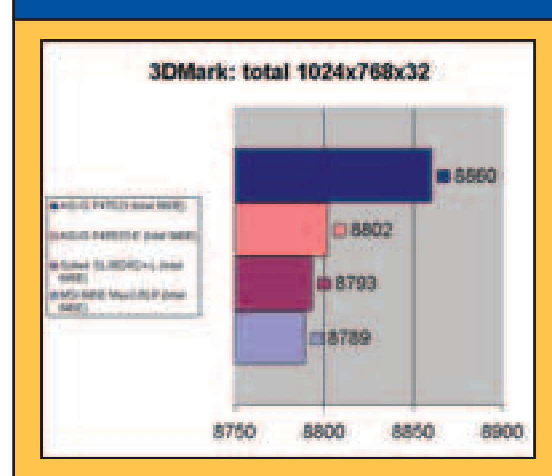
В принципе, с платами ASUS особо напрягаться по настройке системы никогда не приходилось - итак, все настроено на высокую производительность и безглючную работу. Однако оверклокеры с ASUS P4B533-E тоже найдут общий язык. К их услугам разнообразные перемычки и блок DIP-переключателей для выбора

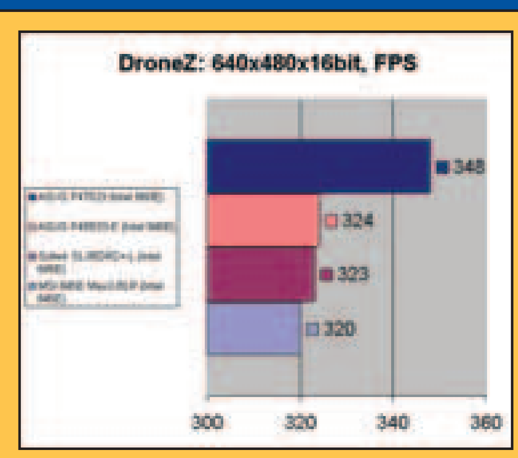


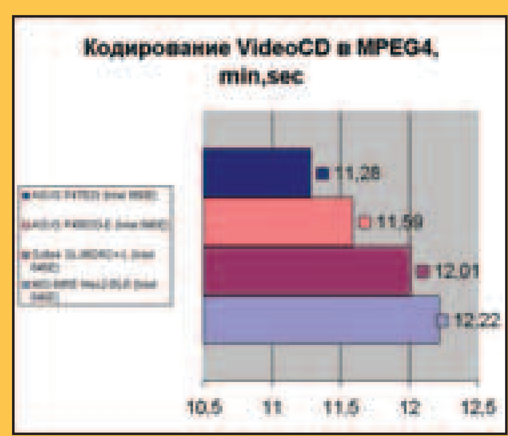
ЛУЧШИЕ МАМЫ НА СВЕТЕ

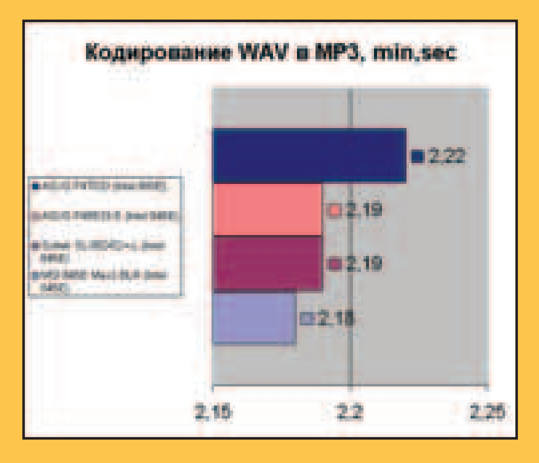
p0r0h (p0r0h@real.xakep.ru)

Тесты

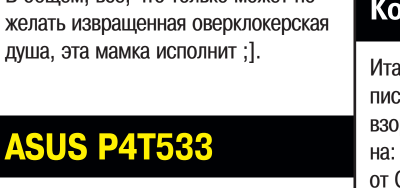








частот шин CPU, AGP, PCI, тонкого изменения напряжения и т.д. Причем, если разбираться с перемычками напрягает, то в BIOS'е тоже доступно множество богатых настроек. В общем, все, что только может пожелать извращенная оверклокерская душа, эта мамка исполнит ;].



ASUS P4T533

Еще одна топ-модель от ASUS. Только на этот раз основанная на другом чипсете - i850E с поддержкой памяти RIMM. Ну, а в остальном она весьма схожа со своей младшей сестренкой ASUS P4B533-E. Однако и у P4T533 есть особой шарм и очарование.

Комплектация

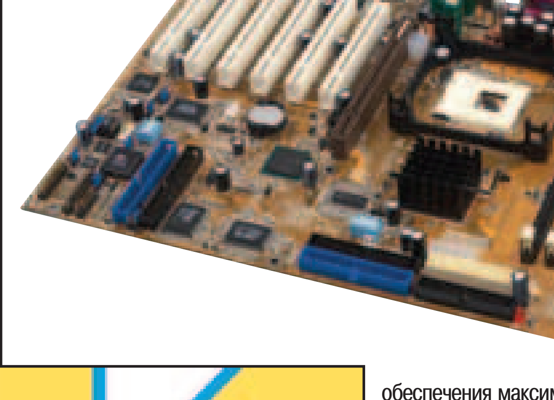
Итак, коробка с завлекающими надписями открыта, и пристальному взору открывается следующая картина: модуль памяти RIMM на 512 МБ от Самсунга, доки и инструкции, три кабеля ATA66/100/133 и один ATA33, шлейф для дисковода, сидюк с дровами и софтом, планка с дополнительными USB 2.0 разъемами, наклейка со схемой и джамперами платы, а также незаменимый пакетик с перемычками :].

Характеристики

ASUS на этот раз доверилась чипсету i850E, а, следовательно, и памяти RDRAM. Насколько оправдан этот шаг, нам еще предстоит узнать, а пока посмотрим на остальные спецификации: поддержка 533 МГц шины, 2 слота под RIMM (в одном из них установлена специальная заглушка для корректной работы прилагаемого модуля памяти), AGP Pro, 6 слотов PCI, порты ввода/вывода - 2 COM/ LPT/ 2 PS/2/4 USB 2.0 плюс 2 USB 1.1. Контроллер Promise PDC20276 обеспечивает поддержку ATA 133 и RAID, а C-Media 8738-MX вывод качественного шестиканального звука. В общем, с такой мамашей можно легко замутить самую крутую тачку и еще долго ловить завистливые взгляды приятелей.

Настройка и разгон

Было бы странно, если бы ASUS не позаботился об оверклокерах и о любителях поковыряться в настройках. Вот и на этот раз ASUS P4T533 предоставляет богатый арсенал для обеспечения максимальной производительности. В наличии имеются блоки DIP-переключателей для изменения частот и напряжения. Причем в БИОСЕ можно изменять частоту системной шины с шагом в 1 МГц, а также вольтаж на камень и другие девайсы с шагом в 0.025 В. Там же доступны настройки для оптимизации работы памяти, а в случае каких-либо «железных» конфликтов (что маловероятно) на помощь придет ручное распределение прерываний.



p0r0h@real.xakep.ru

Шпионские штучки

Обзор цифровых диктофонов

S/N:KJ1 AA007

Тестируемое оборудование ты можешь приобрести, заказав по телефону или через интернет
www.bousheron.ru
www.audiomarket.ru или 363-01-00
www.21vek.ru или 790-31-17

Olympus DM-1

Беря эту вещицу в руки, сразу понимаешь, как она эргономична и хорошо продумана. Да и за дизайн разработчикам можно выразить особую благодарность. Особенно, если



учесть, что это диктофон+мп3плейер в одном флаконе. Но обо всем по порядку. Для начала посмотрим, как хорош он именно в качестве диктофона.

Характеристики

- Комплектация: USB-кабель, SmartMedia-карта 64 МБ, наушники, ПО (DSS-player, MusicMatch), документация, чехол, батарейки;
- Жидкокристаллический дисплей;
- Частотный диапазон для стандартной записи (SP) - 300-5000 кГц, длительной (LP) - 300-3000 кГц;
- Разъемы для наушников и микрофона;
- Ресурс батарей - до 11 часов;
- Встроенный динамик;
- Размеры: 109,5 x 50 x 16,7 мм;
- Вес: 86 г.

Запись речи

Записанные сообщения можно распределить по папкам DSS_FLDA, DSS_FLDB и DSS_FLDC. Всего можно сделать около 600 записей, что, думаю, хватит с лихвой. При желании папки можно и переименовать, чтобы придать им более перевариваемый вид. Чтобы вершить свои темные дела, имеются два режима записи - хороший (SP) и похуже (LP). Тот, что похуже, предназначен на 22 часа работы, но качество будет далеким от идеала. Ну, а с хорошим качеством можно поработать в течение 10 часов, что тоже в принципе не мало. Также регулировке поддается и чувствительность - Conference и Dictation. Первая отрегулирована на максимальный режим и будет записывать все, что услышит, от стонов до лая собак :]. Второй режим, собственно, предназначен для близкой диктовки речи (на расстоянии 5-10 см), как раз если нужно затаиться и по-тихому что-то прошептать. Если же шептать ничего не нужно (например, на официальной встрече или на допросе :)), то может пригодиться возможность подключить внешний микрофон или послушать, как идет запись через наушники.

Фишки

Из основных особенностей DM-1 можно отметить наличие специального режима - VCVA (Variable Control Voice Actuator), позволяющего записывать только речь и останавливающего запись, когда ее нет. Таким образом можно существенно экономить память и записать гораздо больше голосовой инфы. Есть и еще один способ экономить память. Для этого нужно нажать кнопку «Record», и тогда запись перейдет в режим паузы. Однако, если пауза задержится больше чем на 10 минут, то DM-1 отключится (не бойся, запись сохранится :)). Самой же полезной и прикольной фишкой у этого девайса, несомненно, является встроенные таймер и будильник. Для их активации нужно всего лишь выбрать нужное сообщение и время его воспроизведения. В связи с этим можно проделать какое-нибудь отличное западло. Например, предварительно записать лай бешеной собаки или страшного волкодава, а потом поставить такой будильничек сладко спящему корешу. Только особо не перестарайся, а то потом придется вместе с обделавшимся приятелем отстирывать постельное белье ;]. Другой фишкой этого девайса является ускоренное прослушивание (для этого нужно удерживать «Play» более одной секунды).

MP3-плейер

В одном из прошлых номеров мы уже достаточно обширно тестировали специализированные мп3-плейеры, но и на фоне них Olympus DM-1 держался вполне достойно. Первое, что бросается в глаза (а точнее, в уши :)), - это приличного вида и качества наушники. Правда, чтобы добиться хорошего звучания композиций, придется немного повозиться с настройками, т.к. заводские чересчур обрезают нижний и верхний спектры частот. Для этого можно просто-напросто отключить все эффекты или по своему вкусу настроить эквалайзер + поиграться с режимом «WOW», усиливающим басы. Также к услугам юзера предлагаются ID3-тэги, отображающее текущий битрейт и название трэка. А наличие встроенного динамика у DM-1 позволит даже послушать свой музон. Правда, хорошую дискотеку под него не замутишь :].

Olympus Voice-Trek V-10

Этот диктофон, конечно, не так крут, как его старший собрат, но и стоит он на порядок меньше. Дополнительных возможностей типа проигрывания мп3'шек у него нет, так что сразу посмотрим, как он справляется со своей прямой обязанностью.

Запись речи

Прежде чем записывать что-либо, необходимо разобраться в менюшках и функциях. Благо, сделать это осо-



бого труда не доставляет. Дисплей радует своей информативностью, а кнопки продуманностью и удобным расположением. Что касается режимов работы диктофона, то их два - с высокой и средней чувствительностью.

Характеристики

- Комплектация: шнурок для ношения на руке, наушники (моно), USB-кабель, документация, ПО;
- Жидкокристаллический дисплей;
- 32 МБ памяти;
- Частотный диапазон для качественной записи (HQ) - 300 - 5800 Гц, стандартной (SP) - 300-4200 КГц, длительной (LP) - 300-1700 КГц;
- Разъемы для наушников и микрофона;
- Встроенный динамик;
- Ресурс батарей - до 19 часов;
- Размеры: 81 x 47,5 x 22,5 мм;
- Вес: 65 г.

Высокочувствительный режим (Lecture) предназначается для записи источника звука, находящегося непосредственно перед диктофоном. Правда, помимо нужного источника к записи добавляются и дополнительные шумы, так что нужно немного подумать и выбрать нужный режим, прежде чем начать свою шпионскую деятельность.

Фишки

Как и у прошлой модели, в Voice-Trek V-10 имеется возможность активизироваться от голоса - VCVA. Только рекомендую перед этим поставить высокочувствительный режим, чтобы диктофон корректно определял, когда идет голос, а когда храп или стоны :]. Ускоренный режим воспроизведения тоже пригодится, особенно если время поджимает и необходимо быстренько прослушать, что там записалось. Файлы, собственно, записываются в три папки: A, B и S (по сто сообщений для каждой). Последняя папка, кстати, дает возможность выбрать и воспроизвести, находящиеся в ней файлы в определенный день и момент времени. Для этого нужно просто выбрать «Alarm» и указать сообщение + время его проигрывания. Возможности этого своеобразного органайзера на этом, впрочем, не ограничиваются и предоставляют еще одну полезную функцию - это напоминание в течение дня о предстоящих делах и грандиозных планах ;].

Olympus VN-1800

Эта модель тоже своеобразная рабочая лошадка, призванная заниматься своим непосредственным делом - записывать речь и делать голосовые заметки. Да и стоит эта лошадка вполне приемлемо.

Запись речи

Работать с этим диктофоном достаточно просто, благо все хорошо продумано и расположено. Как обычно, имеется несколько режимов качества записи - высокое, стандартное и длительное. Длительного режима хватает на два с половиной часа, но качество, сам понимаешь, будет оставлять желать лучшего. Чувствительность также

Характеристики

- Комплектация: две батарейки, шнурок для диктофона;
- Жидкокристаллический дисплей;
- 16 МБ памяти;
- Разъемы для наушников и микрофона;
- Встроенный динамик;
- Ресурс батарей - до 33 часов;
- Размеры: 96 x 39 x 21,5 мм;
- Вес: 60 г.



можно регулировать, выставив ее в высоком или низком режиме. В целом же никаких нареканий качество записи не вызывает.

Фишки

Сразу дает о себе знать отсутствие USB-интерфейса, так что соединение с компом возможно только через линейный вход звуковой карты, и, следовательно, времени на закачку файла потребуется гораздо больше. Впрочем, трудно ожидать многого от недорогой вещицы. А в остальном все на хорошем уровне. Имеется и ускоренное воспроизведение (на 30%), и органайзер, такой же, как у Voice-Trek'ера. В общем, все, что нужно непритязательному юзверю, он получит :].

SAMSUNG SVR-P750

Эта модель, определенно, сразу вызывает симпатию. Изящные формы и вес могут порадовать кого угодно. Весит SVR-P750 всего 26 граммов, по сути батарейка и то тяжелее ;]. А любителям остаться незамеченными очень пригодится дизайн диктофона, который мало чем отличается от обычной ручки. Поэтому с этим девайсом вполне можно записать приватную или секретную инфу, даже особо не пряча его ;].

Запись речи

Теперь посмотрим, как успешно он будет справляться со своими подслушивающими и записывающими функциями. Собственно, управление ими очень удобно и никаких неудобств не вызывает. Записи в хорошем качестве хватит на 250 минут, в посредственном - 470. Все это добро помещается в двух



Характеристики

- Комплектация: 1 батарея AA, наушники, ремешок для ношения на руке, линейный кабель, USB-кабель, ПО, инструкция;
- Жидкокристаллический дисплей;
- Встроенная флэш-память;
- Записываемый диапазон частот: 300Hz - 3.6kHz;
- Разъем для наушников;
- Встроенный динамик;
- Ресурс батареи - до 8 часов;
- Размеры: 17.5 x 149 мм;
- Вес: 26 г.

папках по 198 сообщений в каждой. Чувствительность регулируемая, с возможностью установки в высоком и низком режимах. Нарекание вызывает, пожалуй, недостаточная громкость встроенного динамика. Из-за чего прослушивать, что там наболтали и нашептали, иногда становится проблематично. Правда, тут на помощь приходит идущий в комплекте наушник-затычка :].

Фишки

Этот диктофон может продемонстрировать отличную сноровку при подключении к компу, переписав, например, на него запись на 7 часов 50 минут всего за какие-нибудь 2 минуты. Сразу видно, что возможности USB-интерфейса использовались практически на полную. Чем еще порадовали инженеры Самсунга? Например, технологией VOR. Символично, не правда ли? ;] Ну что ж, зеленый свет дан, будем воровать инфу с помощью функции Voice Operating Record (аналогична активации от голоса). Остается только взять диктофон и идти изменять историю ;].

D-Pro DR-P800

Признаться честно, я никогда раньше не слышал и не видел диктофонов от компании Digital Direction Electronics. Поэтому слишком многого от знакомства с D-Pro DR-P800 не ждал. А зря. Девайсик оказался весьма непростым и интересным.

Запись речи

Разобраться с функциональными клавишами сможет даже слеповатый ламер - кнопок немного, и все они интуитивно понятны :]. Записать можно до 200 сообщений (для их хранения предусмотрены 2 папки), а время общей

Характеристики

- Комплектация: USB-кабель, ПО, наушник, выносной микрофон, аудио кабель, телефонный адаптер, телефонный кабель, две батарейки;
- ЖК-дисплей с подсветкой;
- 32 МБ памяти;
- Записываемый диапазон частот: 500 Гц - 3.5 КГц;
- Разъемы для наушников;
- Встроенный динамик;
- Ресурс батарей - до 16 часов;
- Размеры: 42 x 112 x 18 мм;
- Вес: 61 г.

записи составит 134 минуты для стандартного режима или 548 для продолжительного. Вот только в продолжительном режиме качество записи будет отнюдь не оптимальным, и чтобы разобрать, что там наговорили, может понадобиться не один литр спирта ;]. Также следует отметить отсутствие выбора чувствительности, однако особого недостатка я в этом не вижу, т.к. чувствительности хватало практически в любых ситуациях.

Фишки

С этим девайсом точно не соскучишься, т.к. возможностей для воплощения в жизнь своей богатой фантазии он предоставляет достаточное количество - имеется линейный кабель для записи с аудио техники, телефонный переходник + телефонный кабель (сам догадайся, для записи каких переговоров :), функция VOR (Voice Operated Recording) позволит диктофону самому начать запись, как только он зафиксирует чей-то голос.

Фотокамера

А что делать, если, помимо звуковой информации, необходима и зрительная? Об этом разработчики D-Pro DR-P800 тоже позаботились и дали возможность почувствовать себя реальным папарацци, записывающим обширный компромат. Всего можно нащелкать до 250 снимков с разрешением 640x480, а уже затем перегнать их на свой комп через USB порт.

Конечно, высококачественные снимки сделать не получится, но разобрать, что на них изображено, особого труда не составит.

PC_Zone

ИНТЕРНЕТ-2

Андрей Каролик (andrusha@sl.ru)

ИНТЕРНЕТ 2

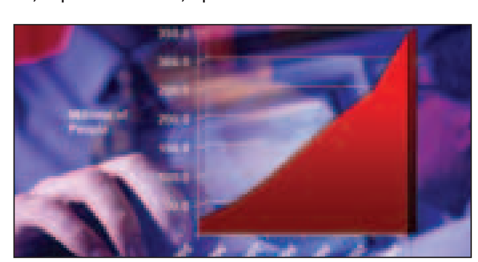
ОБЗОР ПРОЕКТА

Штаты, родившие когда-то ARPANET, не хотят останавливаться на достигнутом и начали строить сеть нового поколения - Интернет-2. Что это такое и зачем делается, ты как раз узнаешь из этой статейки. Пристегнись, полетели :).



Официальное лого

Интернет за последние годы существования скачет в своем развитии круче кенгуру. Начиналось все с военных разработок в 1962-1969 годах, когда только еще сварганили первую экспериментальную сеть - ARPANET (Advanced Research Projects Agency Network). В 1971-1972 годах совместными усилиями INWG (Internet Working Group) родила протокол TCP/IP и спецификацию Telnet (RFC 454). Появился первый Unix :). Ну а дальше все запищало, закрутилось. Скорости росли, но их постоянно не хватало. Магистральная скорость всего за несколько лет (1985-1991) выросла с 56 Кбит/с до 45 Мбит/с (T3). Ну что еще надо людям? Нет, не сидится. Уже в 1992 году разрабатывают идею World Wide Web (WWW), а в 1993-м появился на свет первый браузер - Mosaic. NSF (US National Science Foundation) создает InterNIC - службу, которая занимается регистрацией и учетом лавинно появляющихся хостов. В 1996 году их количество в сети перевалило за 1 миллион штукенций, а в 1999-м зашкалило за отметку в 50 миллионов. Сегодня их, страшно сказать, практически 150 миллионов!



Пользователи Интернета множатся как кролики :)

Содержание Интернета тоже меняется, теперь, кроме текстов и картинок, кругом полно медиа-ресурсов, на которых валяются гигабайты видео - и аудиоматериалов. Но Штаты, родившие когда-то ARPANET, не хотят останавливаться на достигнутом и начали строить сеть нового поколения - Интернет-2. Что это такое и зачем делается, ты как раз узнаешь из этой статейки. Пристегнись, полетели :).

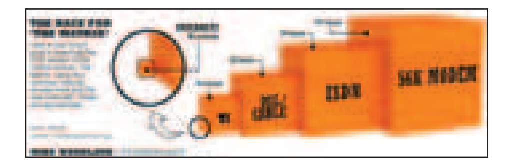
<Низкая эффективность>

Интернет успешно развивается и будет развиваться, но со временем перед Штатами встала проблема - так называемый потенциал решения проблемы PSP (Problem Solving Potential). Под PSP в данном случае понимается эффективность полученной информации из Интернета для пользователя, который решает конкретную задачу. Из-за хаотичного появления кучи малополезных урл-ов обычный Интернет, который

ты юзаешь каждый день, по оценкам аналитиков всегда будет иметь очень низкий потенциал (PSP). В результате уже сегодня стоит острая проблема использования Интернета в профессиональных целях. Другими словами, изначально любой пользователь, используя всемирную паутину, испытывает динамические ограничения на своевременность, достоверность и полноту полученной информации. В первую очередь остро эту проблему испытывает образовательная система в Штатах, широко практикующая дистанционное обучение. Дистанционное обучение ориентировано именно на то, чтобы обеспечить обучаемому определенный уровень PSP. То есть дать ему в полном объеме то, что он ищет, чтобы он не копошился впустую. Проблема увеличения эффективности использования Интернета (PSP) послужила одной из основных причин для организации нового проекта - закрытой сети Интернет-2. То есть физики, биологи, медики и прочие большеголовые дядьки хотят вернуть себе то, что они имели несколько лет назад. Ведь Интернет изначально делался для военных и ученых, а сегодня он используется для целей, далеких от научных исследований. И выглядит он сегодня не как всемирная паутина, а как всемирная помойка всякой всячины :). Простой пример - я убил просто кучу времени, чтобы накопать свежую, достоверную, полную и одновременно интересную информацию для этой статьи. Ничего лучше, чем перевести в лоб единственный и неповторимый сайт на забугровом языке о новом проекте, а потом догоняться самостоятельно, что же они имели ввиду, в результате я не придумал. Может мне как раз не хватало Интернет-2 :)?

<Нехватка мощностей>

Для некоторых специфических технических задач уже не хватает даже существующих мегабитных каналов. И вторая основная задача нового проекта - повышение скорости передачи информации с современной мегабитной до гигабитной. Скорость передачи данных вырастет аж до 10 Гбит/с! Для примера, за 1 секунду по Интернет-2 можно перессдать все 30 томов Британской энциклопедии, что в 100-1000 раз быстрее, чем по каналам обычного Интернета. Знали бы они, как долго придется утягивать эти 30 томов простому парню из деревни Лошки по обычному мопеду :).



Разница заметна невооруженным глазом…

Но закрытая сеть Интернет-2 не рассчитана на обычных пользователей, и ее внедрение будет производиться параллельно традиционному Интернету, так что ты на собственной шкуре прочувствуешь мегаскорость не скоро. Но для чего нужны эти сверхскорости? Для проведения, к примеру, видеоконференций в реальном времени, которые будут служить виртуальным пространством для обсуждения университетами разных стран насущных проблем, не вставая со своего любимого стула. Обычный Интернет не дает такой возможности вовсе или накладывает ограничения на скорость и качество передаваемого поточного видео и звука. Результат - маленькое пищащее окошко с плохим разрешением. Более-менее приемлемые результаты дает только локальная сеть. Интернет-2 позволяет делать конференции с эффектом присутствия, проецируя изображение на специальном оборудовании и используя одновременно несколько проекционных камер. Проблемы со скоростью передачи данных уже отпадают, остается только разработать приложения для обработки и визуализации поступающей информации. Уже сегодня ведутся активные и весьма успешные разработки 3D-конференций, которые в будущем должны вытеснить обычные конференции.

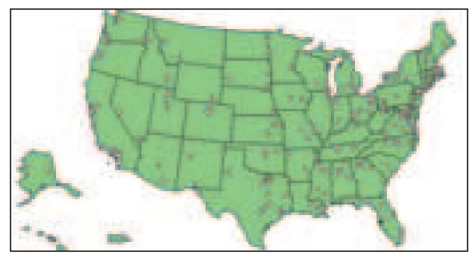


Не за горами и интерактивный Quake по Инету ;)

То, что раньше ты видел только в фантастических фильмах, сегодня постепенно становится реальностью. Кроме видеоконференций, в науке существует проблема мощных вычислительных средств, которые доступны далеко не каждому. Частичное использование их дистанционно возможно уже сейчас, но только с увеличением скорости передачи информации можно будет их эффективно использовать на все 100%. Ученым и студентам уже не нужно будет ждать, пока персоналка станет париться полдня, высчитывая требуемые навороченные формулы. Они просто перешлют исходные данные на более мощные вычислительные средства и практически моментально получат искомый ответ. Но есть небольшая проблемка - пока не будут модернизированы сети университетских городков, выигрыш в скорости, обеспечиваемый новой опорной сетью, останется минимальным. Более того, пользователи только теперь начинают разрабатывать прикладные программы, которые будут способны использовать эту сверхскорость. Но основные затраты на необходимую модернизацию ПО и аппаратуры дает государство в виде грантов, а гранты у них не такие, как наша стипендия :). Поживем - увидим.

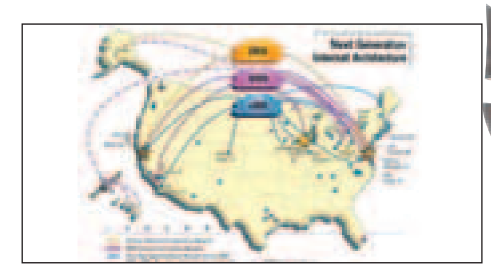
<Создание проекта Интернет-2>

Активно базарить о проекте Интернет-2 стали только сейчас, потому что он набрал обороты и пошел в гору. Уже сейчас (данные на февраль 2002 года) проект поддерживает и внедряет в Штатах 191 университет.



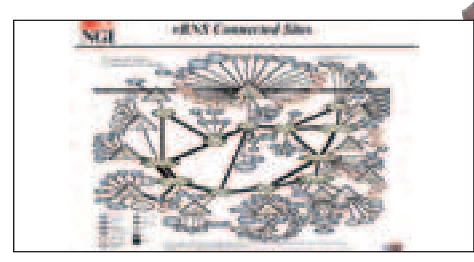
В феврале 2002-го проект поддерживает 191 институт

Но изначально о необходимости его создания заговорили еще в октябре 1996 года, когда в Чикаго собрались на встречу представители 34 университетов и подняли этот вопрос. Попив минералки и почесав лысые затылки, они решили строить проект своими силами с ежегодными инвестициями со стороны каждого участника в размере 500 тысяч зеленых. Позже, в феврале 1997 года, новым проектом заинтересовался и поддержал сам президент Штатов Билл Клинтон. Он решил в дальнейшем скрестить Интернет-2 с правительственным проектом NGI (Next Generation Internet), который имеет в основе сходные принципы. Что такое NGI? Это открытый проект (Интернет-2 является закрытой сетью), в основе которого лежит программа создания новых сетевых технологий для федеральных нужд с более продвинутой базой и более высокой пропускной способностью, чем обычный Интернет. Основными задачами NGI являются: создание высокоскоростной сети, получение развитых технологий сетевого сервиса, разработка прикладных программ нового поколения. Минимальная сквозная скорость каналов должна быть от 100 Мбит/с до 1 Гбит/с. Президент Клинтон и вице-президент Гор 10 октября 1996 года толкнули официальную речь о том, что поддерживают инициативу создания Интернета следующего поколения (Next-Generation Internet, NGI), базирующегося на новейших программах исследований и разработок, проводимых в федеральных ведомствах. Эта инициатива направлена на поддержку научных исследований и разработок в области крупномасштабной сети и обеспечение высокоскоростных соединений между основными исследовательскими центрами. Техническую основу реализации NGI составляет высокоскоростная опорная сеть vBNS.



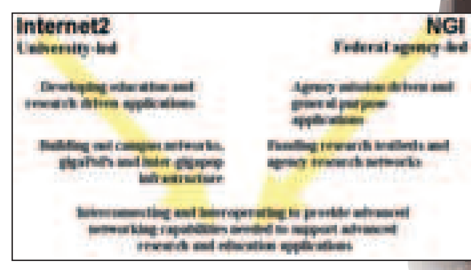
Вот он, Интернет будущего (NGI)

Использование скоростных каналов потребует разработки новых технологий сетевого сервиса. К ним можно отнести новые протоколы передачи данных, отвечающие возросшим требованиям эффективности работы, средства обеспечения безопасности передачи данных, средства для администрирования и управления сетью. Кроме того, создание прикладных программ нового уровня, использующих в полной мере все возможности новых скоростных соединений.



Общая топология vBNS

Примерами могут служить видеоконференции, программы для дистанционного управления физическими экспериментами, программы мониторинга окружающей среды, здравоохранения, телемедицина и т.п. Одним словом, проект Интернет-2 большей частью был похож на проект федералов, и федералы стали его финансировать. Проект Интернет-2, в свою очередь, смог использовать наработки NGI.



Взаимодействие NGI и Интернет-2



PC_Zone

ИНТЕРНЕТ-2

Андрей Каролик (andrusha@sl.ru)

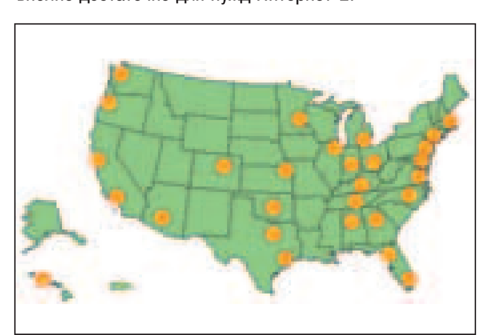
Но в целом Интернет-2 остался самостоятельным закрытым проектом, чтобы не повторить ошибку захламленности современного Интернета, ради чего, собственно, и создавался.

Скорость передачи данных вырастет аж до 10 Гбит/с! Для примера, за 1 секунду по Интернет-2 можно передать все 30 томов Британской энциклопедии, что в 100-1000 раз быстрее, чем по каналам обычного Интернета.

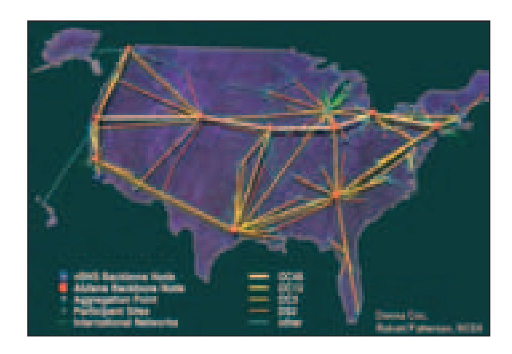


<Структура Интернет-2>

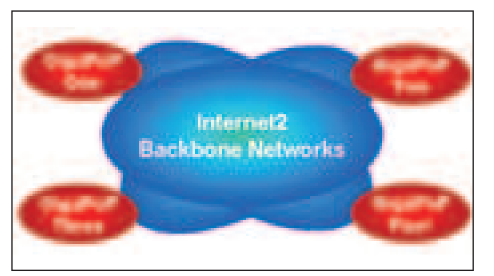
Что, собственно, Интернет-2 представляет собой сегодня и какова его общая структура? Вся сеть Интернет-2 состоит из узловых точек - GigaPoPs (gigabit-capacity points of presence, с пингвинского точки доступа гигабитной мощности). На данный момент таких точек всего 28 штук. Узловые точки связаны общей магистралью, которая обзывается у них Internet2 Backbone Networks. Непосредственно к узловым точкам через оптоволокно цепляются университеты, всевозможные исследовательские сетки и обычный Интернет. Общая магистраль держится на волоконно-оптической магистральной сети Abilene стоимостью 500 миллионов зеленых. Она была разработана University Corporation для организации UCAID (Advanced Internet Development) при участии таких гигантов, как Qwest Communications, Nortel Networks, Cisco Systems и Indiana University. Сеть Abilene функционирует со скоростью до 2,4 Гбит/с, что вполне достаточно для нужд Интернет-2.



Узловые точки GigaPoPs



Internet2 Backbone Networks



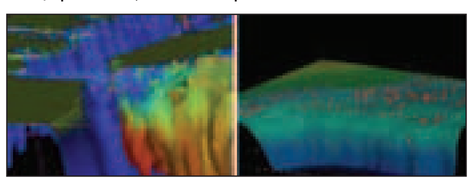
Internet2 Network Architecture

Переход на новые скоростные каналы потребует новых протоколов маршрутизации, так как использование старых протоколов будет сильно уменьшать их реальную пропускную способность. Что касается протокола IP, то его тоже переработали, так как всего может существовать около 4 млрд. четырехбайтовых IP-адресов, при этом некоторые комбинации цифр не являются реальными адресами и служат для специальных целей. Поскольку сейчас отдельные IP-адреса требуются не только компьютерам, но и различным устройствам: принтерам, средствам бесперебойного питания UPS и т.п., то такая цифра вовсе не кажется слишком большой. Поэтому сейчас уже разработана новая версия протокола IP, названная IPv6 (IP version 6). В этом протоколе количества цифр в IP-адресе увеличено. Этот протокол и будет использован в дальнейшем в Интернет-2.

Если ты заинтересовался материалом, то можешь самостоятельно полазить по www.internet2.edu, подгрузив электронный англо-русский словарик.

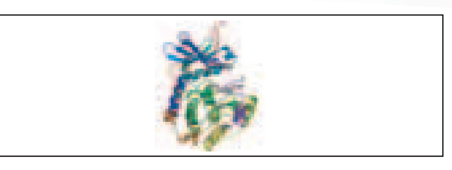
<Приложения для Internet2>

Уже сегодня для Интернет-2 созданы кучи приложений, которые эффективно используются американскими институтами в процессе обучения. Некоторые из них очень любопытные и специфические, вот некоторые из них:



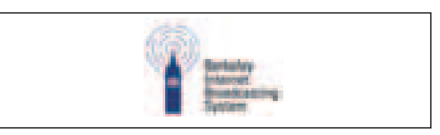
Cave5D

Cave5D (www.ccpo.odu.edu/~cave5d/homepage.html) Электронная лаборатория визуализации. Виртуальная среда, которая позволяет полученные данные просматривать, визуализировать, анализировать и преобразовывать в реальном времени. В программе имеется куча настроек. Позволяет получить непрерывную визуализацию дистанционных процессов, данные о которых будут передаваться через сеть.



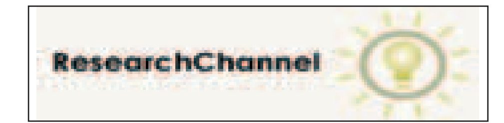
MICE

MICE, Molecular Interactive Collaborative Environment (http://mice.sdsc.edu) Еще одна среда сложной визуализации, ориентированная на молекулярный анализ. Все существующие методы позволяют делать визуализацию только статических данных или двухмерных сред. Эта программулина позволяет визуализировать в реальном времени, исследовать и воздействовать на макромолекулы в трехмерной среде. Движок построен на Java3D.



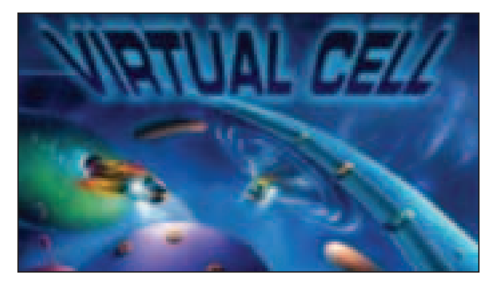
BIBS

BIBS, Berkeley Internet Broadcasting System (http://bmrc.berkeley.edu/bibs) Интерактивная телевизионная система, которая позволяет дистанционно обучаться. Разрабатывалась в данном случае специально для студентов Беркли. Поддерживает сотни одновременно работающих программ, включающие аудио, видео и данные. Позволяет дистанционно он-лайн проводить лекции и семинары с большим количеством пользователей одновременно.



ResearchChannel

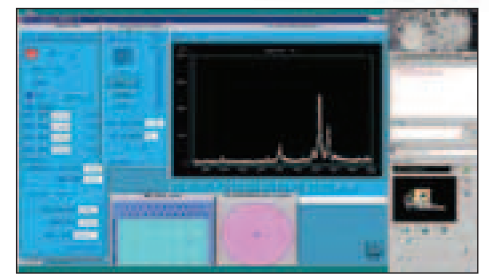
ResearchChannel (www.researchchannel.com) Проект сразу нескольких университетов, направленный на продвижение канала качественного видео и радиопередач через Интернет. Позволяет просматривать онлайновые проекты или архивные ролики. Используется для прямой связи и передачи новостей, исследований, открытий и просто дистанционного общения между университетами.



The Virtual Cell

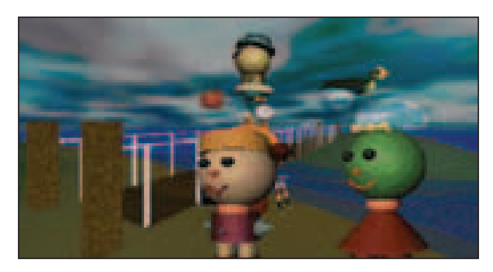
The Virtual Cell (www.ndsu.nodak.edu/instruct/mcclean/vc) Эмуляция среды, в которой студенты могут изучать структуру и функции клетки. Взаимодействие происходит в реальном времени. Можно наглядно изучать жизнедеятельность любой клетки. Ролевая игра, одним словом :). Движок построен на VRML.





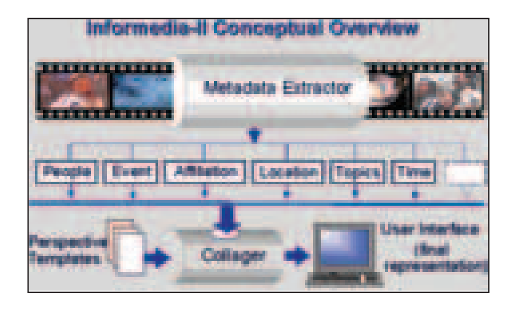
Mass Spectrometry

Mass Spectrometry (www.udel.edu/topics/internet2/proj/maldi) Универсальный спектрометр. Позволяет разнести дорогое оборудование в лаборатории и исследователей, которые дистанционно из любого места могут получать данные опыта, отправив в лабораторию нужные образцы.



Tele-immersion

Tele-immersion (www.evl.uic.edu/spiff/calvin) Среда разработки окружающей виртуальной среды. Позволяет участникам, расположенным дистанционно по отношению друг к другу, создавать виртуальные миры, в которых они могут общаться. Широко используется также для организации видео- и телеконференций.



The Informedia Digital Video Library

The Informedia Digital Video Library (www.informedia.cs.cmu.edu) Цифровая информационная видеобиблиотека. Предоставляет автоматическую индексацию, навигацию, визуализацию и поиск для обучающих, информационных и развлекательных данных. Может автоматически распознавать и отличать звуки, картинки, видео и прочее. Есть возможность обучать систему.

<Вердикт всей байде>

Интернет-2 очень перспективный проект и даст множество новых возможностей, которые не может дать обычный Интернет. Виртуальная лабораторная работа на другом континенте станет обычным делом. Возможно, в ближайшем будущем врач тебя сможет осматривать прямо дома и ставить диагноз на расстоянии, а ученые смогут сделать много новых открытий и изобретений в результате дистанционного и эффективного использования доступных мощностей. Конечно, читая этот материал, обидно, что мы постоянно отстаем от тех же Штатов по вычислительной технике и коммуникациям лет на 7-8. Так что пока остается только смотреть со стороны и глотать слюни. Но рано или поздно волна новшеств докатится и до нас. А уже сейчас, к примеру, есть реальные предложения Владивостоку со стороны Калифорнийского университета в создании спутникового канала на средства гранта НАТО. На эти средства планируется приобрести коммуникационное оборудование и развернуть систему доступа к информационно-образовательным ресурсам. Это даст возможность связать образовательную сеть Приморья с Калифорнийской университетской сетью. А так как Калифорнийский университет входит в проект Интернет-2, то это реальные шансы в будущем подрубиться и к проекту Интернет-2. Реализация этого проекта рассчитана на 2 года, так что все впереди. Если ты заинтересовался материалом, то можешь самостоятельно полазить по www.internet2.edu, подгрузив электронный англо-русский словарик.



TIPS&TRICKS

Если у тебя машина тарахтит и воет волком - выкинь ты ее подальше, нам такая не нужна! А если серьезно, этот Tips&Tricks написан для тех, кто до сих пор мучается с 486DX, Pentium 100 и иже с ними. Короче, не знаю, как там у тебя, а меня уже порядком достала моя тачка P-166, 32 Mb, которая постоянно шуршит своим винтом и жужжит вентилятором, как АЭС какая-нибудь... Но выход есть всегда! И мы оптимизируем твою микроЭВМ по полной ;). Для начала убери все феньки со своей Винды: всякие wallpaper'ы, крутые иконки, курсоры, заставки и т.д. Эта братия тормозит твою тачку не по-детски. Всякие окошечки, пимпочки и т.д. - все делай по дефолту! Идем дальше: насчет софта, не ставь всякие ресурсоемкие приложения, ищи альтернативу! А если ее нет - напиши свою прогу ;). Один вопрос: ты используешь AVP/Photoshop 6.0/MS OfficeXP/WinMe/CorelDraw v999? Если да - иди-ка ты подальше удалять их, потому что данные индивидуумы на фиг тебе не нужны! Не пытайся гнаться за техническим прогрессом, не качай последние версии, если тачка у тебя не P4/Athlon. Такой софт для тебя unreal, ищи альтернативу. Кстати, вот тебе и альтернатива вышеприведенному списку: Dr.Web/Photoshop 5.0/MS Office 97/2k/Win98/95/3.1/1.0 ;) (а лучше Линух)/Freehand 9. Особо не загружай проц, убивай резидентов и проги, которые любят посидеть в трее. Лично у меня всего одна прога в трее - TrayService. Наверняка ты про такую и не слышал, а зря, ента штука позволяет быстро добираться до нужных тебе папок, чистить темповые папки, кэш, открывать сидюки, взрывать мониторы... Все это можно посадить на "горячие" клавиши; сама прога написана на VC с использованием WinAPI, поэтому отжирает памяти она немного. И весит - ~70Kb. Иди, качай ;) - http://nocode.km.ru/download.htm. Ну вот, вроде бы и все. Напоследок хочу сказать, что главный принцип владельца доисторической машины - у тебя все получится, и за такой тачкой можно работать, поверь мне. И избегай как можно больше всякой мультимедии, архивов divx и mp3. Вообще, ставь себе *nix, там консоль не тормозит ;). Удачи!

Дмитрий Алексеенко
(dmitri@pisem.net)

PC_Zone



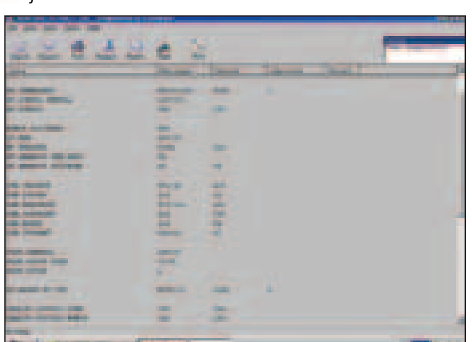
WINPOINT - FIDONET НА ЛАДОНИ

Скрыпников Сергей 'aka' Slam
(sergey@soobcha.ru, 2:5058/103.777)

СОФТ ДЛЯ НАЧИНАЮЩЕГО ФИДОШНИКА

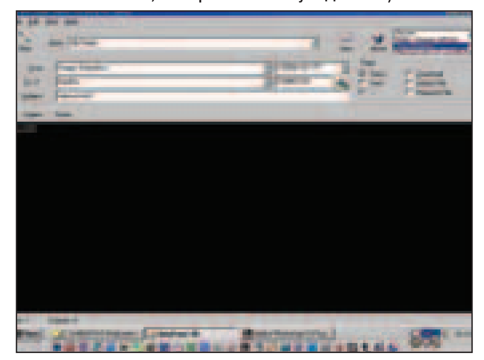
Помнится, в 11 номере за 2001 год я рассказывал тебе, что же такое это самое FIDO. Так вот, думаю, что ты прочитал и тебе понравилось =), и ты наверняка захотел подключиться, но для этого нужно иметь необходимый софт (как получить пойнта, ты тоже знаешь). Так вот, есть такая волшебная программка, которая называется WinPoint. Это как бы 3 в 1 - и тоссер, и мейлер, и редактор сообщений. Тебе не нужно больше настраивать отдельно каждую программку а потом геморроиться, чтобы они еще вместе работали, теперь тебе достаточно ввести пару значений, и вся программа настроена, главное - не забывай, когда можно звонить твоему боссу :-).

Итак, приступим.
Бегом нahttp://www.schenksmir.de/wp/english/ или на http://winpoint.narod.ru/, и качай оттуда WP версии желательно не ниже 1.78 (а именно про нее я буду тебе рассказывать). Скачал? Так, давай сникерсни и распаковывай, запускай. Программа начнет последовательно спрашивать твое имя, фамилию (обязательное условие подключения к ФИДО - использование настоящих имени и фамилии, никаких никнеймов - "пережитков Интернета"), твой адрес в сети (который выдал тебе босс), номер телефона босса, и так по мелочи. Естественно, как и все шаровары, WP будет тебе надоедать и просить у тебя денег, но я-то знаю, что лишних у тебя нет, а если и есть, то ты их не отдашь, так что специально для таких, как ты, САМ АВТОР решился на то, что для наших она будет фриварной:
User: **Freeware**
Key : **005A7470**



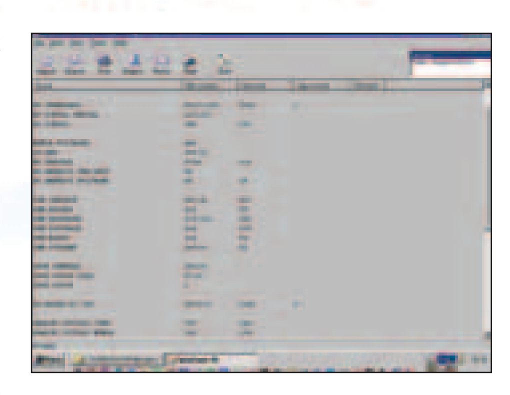
Так выглядит WinPoint

Теперь самое время подписаться на эхоконференции (ведь ты не собираешься пользоваться только почтой?). Для этого существует робот AreaFix. В общем, делай так: заходи в WP в раздел NetMail (здесь будут храниться письма, пришедшие лично тебе), нажимай кнопочку NEW, появится окно, там в поле To: вводи "AreaFix" (без кавычек, есесно) и адрес твоего босса, т.е., например, если адрес у тебя 6:6666/666.666, то ты должен ввести 6:666/666, в поле Subject пиши свой пароль. Теперь, непосредственно в самом теле письма, пиши %LIST (этой командой ты говоришь роботу, чтобы он выслал тебе список доступных эх, которые держит твой босс), нажимай Save, потом Esc (на клавиатуре), посмотри наверх и увидишь там кнопочку POLL, нажимай на нее, потом нажимай на кнопочку Call - все, если у тебя нормально настроен мопед, то WP дозвонится и отошлет почту. Подожди минут 10-15 после дисконнекта и звони еще раз. На этот раз для тебя должна быть почта, она сама скачается. Лезь в раздел НетМыло, там ищи новое письмо, дабл клик по нему, и оно перед тобой. Ты увидишь список доступных эх с их описанием, теперь бегом за ручкой (карандашиком, маркером, губнушкой) и листочком и записывай названия тех эх, которые тебе больше всего нравятся (надеюсь твой босс будет держать RU.SEX и RU.HACKER =)). Записал? Молодец, затем создавай новое письмо (надеюсь, ты уже научился, если нет, то перечитай все сначала), опять пиши его к AreaFix'у, но в теле письма пиши:
+vot.takaja.exa
+i.vot.takaja
Естественно, после "+" (а "+" означает, что ты хочешь подписаться на эху, "-" - соответственно - отписаться) ты должен писать названия эх, ПО ОДНОЙ В КАЖДОЙ СТРОКЕ!
Сохраняй, звони, жди (теперь уже поболе, может и 10 минут, а может и сутки =)).
Пока ждешь, беги в настройки BBS, там ставь new areas -> create automatically, этим самым ты приказываешь WP, чтобы при поступлении хотя бы одного нового письма с неизвестной ему пока эхи он создавал новый раздел с названием этой эхи (ну, типа фильтра в The Bat!). Если тебе потом не понравится эха, то сначала от нее отписывайся, жди примерно сутки (т.е. жди подтверждения отписки), выделяй арию, нажимай Ctrl+Delete - все, теперь ты ее не увидишь :-).



Посылаем запрос AreaFix'у

Если тебе не понравился встроенный мейлер, то делай следующее: сначала отдельно настраивай EMSI-mailer для работы, затем в настройках WinPoint прописывай узлы своих боссов в разделах "Fidonet" и "BBS", не забыв в последнем обязательно заполнить поле "Netcall", прописав в нем строку для запуска вышеупомянутого EMSI-mailer'а. Заключительный этап заключается в том, что WinPoint и EMSI-mailer должны обязательно использовать общие каталоги Bink Style Inbound/Outbound, в WinPoint это реализуется путем заполнения полей "Settings\More\Folders\Inbound" и "Settings\More\Folders\Outbound" соответственно. Теперь забрать почту у своих боссов можно либо нажав кнопку "Poll" на главной панели инструментов WinPoint, либо запустив внешний EMSI-mailer самостоятельно, что в конечном счете одно и то же.



Настраиваем WP

Надеюсь, ты уже получил новуюпачку писем с новых эх? Да? Очень хорошо, теперь я расскажу тебе, как правильно настроить чтение писем. Для того чтобы при сохранении письма не были испорчены автозаменой на "ид" и "ае", нужно сделать одну вещь. Заходи settings>areas-> название нужной эхи и снимай флажки convert gGermanumlauts и convert Я to ss.
2) Для того чтобы не исчезала Н (самая частая проблема начинающих фидошников), поставь флаг convert Convert Russian H.
3)Если хочешь нормально перелистывать письма (ну, что пришло, то и смотришь), поставь sorted by imported, тогда все будет ОК.
Для нормальной работы нужно установить пойнтлисты, это делается следующим образом: скачивай пойнтлист у босса, устанавливай значения файлов в settings->lists, нажимай file->process nodelist. Для поиска нажимай F9.

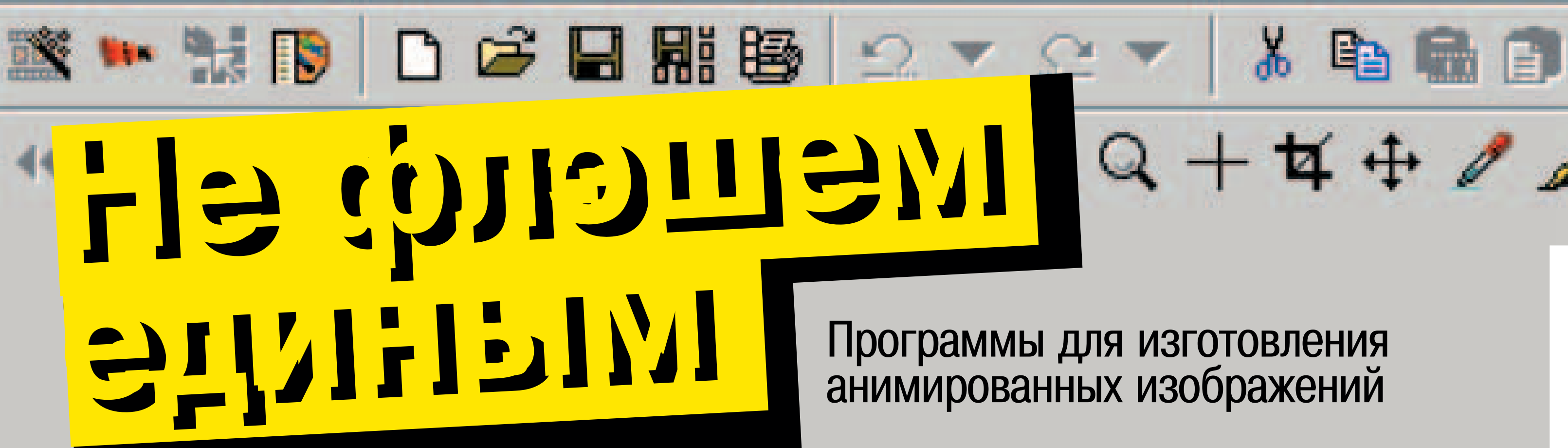
Думаю, для нормальной работы с почтой и эхоконфами этого тебе вполне хватит. Если что-то непонятно, то мой мыл всегда открыт для тебя. Работу с файлами мы разберем в следующий раз.

TIPS&TRICKS

Хочу поделиться советом, как без firewall-а обнаружить атаку на комп. Если у тебя установлена "служба доступа к файлам и принтерам сетей Microsoft", то все получится. Значит так, не вставляя дискету, заходишь в свойства диска А:, далее выбираешь вкладку Доступ, затем отмечаешь "общий ресурс", в поле "сетевое имя" пишешь "Windows", "тип доступа" - "только чтение". В принципе, все готово, но для пущей уверенности в том, что наивный ламер действительно принял все за правду, надо создать где-нибудь, в укромном местечке, на винте папку, назови ее, например, "firewall". В этой папке создай две подпапки, одну с названием "Program files", а вторую "Мои документы". После сделай ту же процедуру, что и с А:, только сетевые имена дай соответствующие названиям этих папок. Все, самодельный firewall готов. Как только злобные хакеры захотят скачать твои PWL-ки, флопак поднимет тревогу :).

[MDG]RedpaX. redpax@e-mail.ru

Horrific smirnandr@mail.ru www.cyd-soft.com/vr-online



Не флэшем единым

Программы для изготовления анимированных изображений

С появлением Flash5 все почему-то ринулись создавать свои сайты и баннеры именно с помощью него. Такое ощущение, что других программ просто не существует. А как же старые добрые GIF-аниматоры? Неужели они должны улететь за борт? Ни в коем случае!!! Они жили, живут и будут жить!!!

<ПОЧЕМУ FLASH НЕ ВСЕСИЛЕН?>

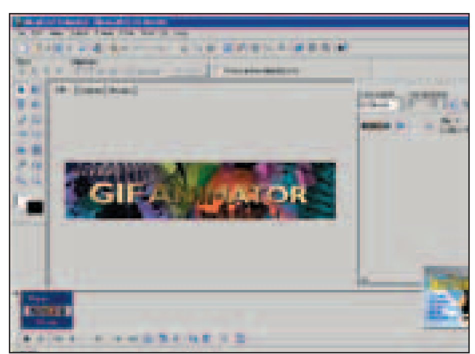
Я не буду здесь разводить большую лекцию, потому что передо мной не стоит задача объяснения графических форматов, но и умолчать я тоже не могу. Поэтому я коротко покажу, когда применение FLASH для создания графики в WEB неэффективно. С помощью FLASH можно создавать векторную графику для WEB. Некоторые считают, что картинка в векторе занимает в несколько раз меньше места, чем в растре. Это правда, но не на все 100%. Вектор эффективен только если картинка очень простая и содержит маленькое число цветов. В остальных случаях вектор прожорлив. Если картинка сложная и насыщена цветами (например, фотография), то желательно сжимать ее с помощью алгоритма Jpeg. Он сдавливает файлы с потерей качества, но при большой насыщенности картинки цветами это незаметно.

Если картинка содержит мало цветов, но изображение сложное, то тут лучше подойдут GIF-файлы. Этот формат удобен не только маленьким размером результирующего файла, но и тем, что может содержать анимацию. Вообще, GIF-формат я считаю наиболее универсальным. Если количество цветов очень мало, то размер GIF файла тоже будет очень маленьким. Сложность сцены тут не играет особого значения. Конечно же, если картинка будет сложной, то и размер файла будет больше, но не намного.

<ULEAD GIF ANIMATOR>

www.ulead.com/
Размер: 11 метров

Эту программу я считаю лучшей для сборки GIF-файлов. Ее интерфейс очень прост и удобен. Я бы даже сказал, что он напоминает Photoshop. С другой стороны, он очень перегружен, и обладатели маленьких мониторов могут столкнуться с проблемами нехватки рабочего пространства. При сборке анимации ты так же, как и в Photoshop-е, сможешь оперировать слоями. Каждому слою можно назначить свою прозрачность и даже степень прозрачности. Но я не советую тебе создавать полупрозрачные слои, потому что тут сразу начинает работать смешение цветов, что приведет к заметному увеличению размера файла.



Ulead GIF Animator

Если фильтров в стандартной поставке я не увидел (их нужно устанавливать отдельно), то вот эффектов сколько угодно. С помощью этих эффектов можно в пять сек оживить любую статичную картинку. Если ты создаешь анимацию не для WEB, то ты по достоинству оценишь все эффекты. Но если ты хочешь создать анимированный баннер, то проматеришь разработчиков Ulead, их родителей и всех их родственников. Большинство эффектов увеличивает размер анимации в разы. Баннеры в 50 кило не позволит у себя разместить ни одна из баннерных систем. Так что эффектами рекомендуется пользоваться осторожно.

Если заглянуть в помощь Ulead GIF Animator и почитать имена разработчиков, то можно язык сломать :). Это и не удивительно, ведь прогу написали тайваньские ребята (второй адрес фирмы в Инете http://www.ulead.com.tw/). И все же собирать анимацию в Ulead GIF Animator очень удобно. С помощью этой тулзы можно без проблем превратить в GIF даже видеофайлы. Только не вздумай открывать свой любимый фильм "Матрицу", а то компьютер моментально сдохнет.

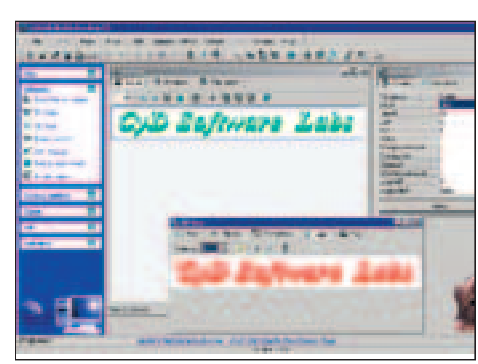
<CYD GIF STUDIO PRO>

www.cydsoft.com
Размер: 3,6 метра

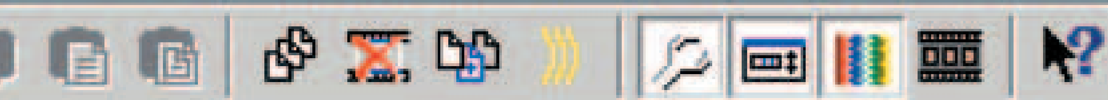
В моей проге так же есть эффекты. Они попроще, чем в Ulead GIF Animator, но зато они не так сильно увеличивают размеры файла. Если создать анимацию с помощью любого эффекта на 5 кадров, то файл получится приемлемых для любой баннерной системы размеров.

В проге также удобно реализованы возможности управления кадрами - прозрачностью и длительностью проигрывания отдельных фреймов.

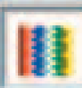
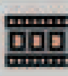
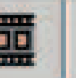
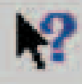
Среди мастеров лучшим считается "3D Text", с помощью которого можно создавать кадры, содержащие трехмерный текст. Такие кадры получаются не фотографического качества, зато не сильно увеличивают размер файлов. Вообще, CyD GIF Studio Pro построена так, чтобы любая из ее функций не сильно влияла на размер анимации. Прога надежно работает только в Windows 2000. На остальных тоже работает, но на некоторых системах с Windows 98 прога просто сыпется ошибками :(. Такие системы встречаются редко, но все же я обязан предупредить....



CyD GIF Studio Pro

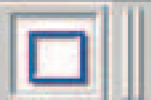





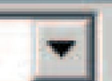










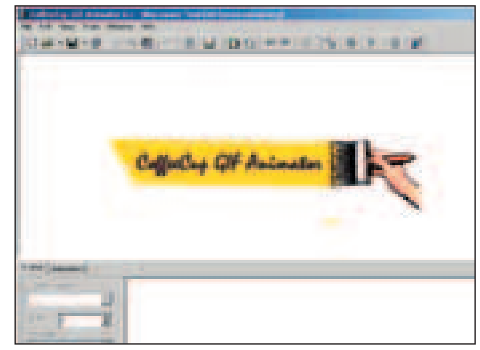





<COFFEECUP GIF ANIMATOR>

www.coffeecup.com
Размер: около 2 метров

Честно сказать, первые проги этой фирмы меня покорили. Но GIF аниматор меня убил. Такой лажи я не ожидал от такого солидного производителя. Аниматор действительно простой, и с ним можно создать практически любую анимацию. Но найти какую-нибудь изюминку мне не удалось. Оптимизация не на самом лучшем уровне. Фильтры и эффекты просто отсутствуют.



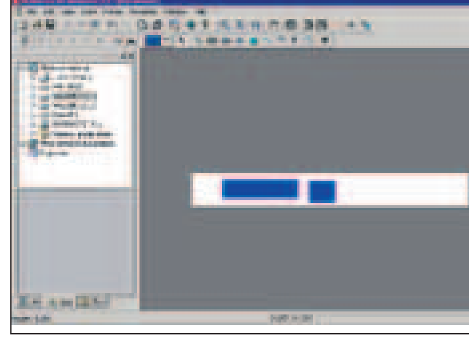
CoffeeCup GIF Animator

CoffeeCup GIF Animator - это простенький аниматор для создания простеньких GIF файлов. Ничего особенного он собой не представляет, поэтому я поражаюсь, почему его скачивает наибольшее количество народу на download.com?

<BABAROSA GIF ANIMATOR>

www.liatro.com/
Размер: около 800 кило

Еще один простенький и маленький аниматор. Я бы позиционировал его как удобное средство для создания GIF файлов. Все примитивы, которые ты здесь рисуешь, создаются в векторе, и поэтому файлы очень удобно редактировать и превращать в движение. Но этот же вектор не позволяет использовать эффекты и фильтры к кадрам, потому что такое возможно только с растром. Нормальная оптимизация тут также невозможна. Так что для сжатия анимации придется завести что-нибудь другое.



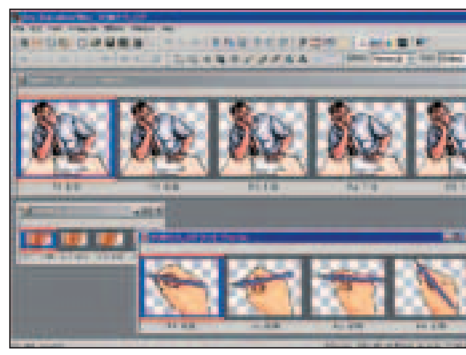
Babarosa Gif Animator

На первый взгляд программа очень простая и маленькая, но некоторые вещи в ней создавать намного удобнее, чем даже в тяжеловесном Ulead GIF Animator. Так что для создания анимации не помешает хранить этого жучка на своем винте.

<JASC ANIMATION SHOP. >

www.jasc.com/
Размер: почти 12 метров

С помощью этой программы ты будешь работать с анимацией в виде растра. Никаких возможностей для оптимизации тут нет. Эффекты очень сильно увеличивают размер файла, поэтому не советую использовать их для WEB-анимации. Никаких особенностей в программе нет. Короче говоря, на первый взгляд это полный отстой. Тогда зачем же нужна тебе эта тулза? В ней есть возможность работы с такими форматами, как FLC, FLI, AVI, ANI и даже MNG. Большую часть моего обзора заняли проги для создания GIF-анимации. Оно и понятно, ведь первое, о чем думает любой продвинутый мен, так это о создании собственной страницы в Инете. Но нельзя же забывать про такие форматы анимации, как FLC и FLI. Они достаточно распространены и за все время своего существования не потеряли популярности.



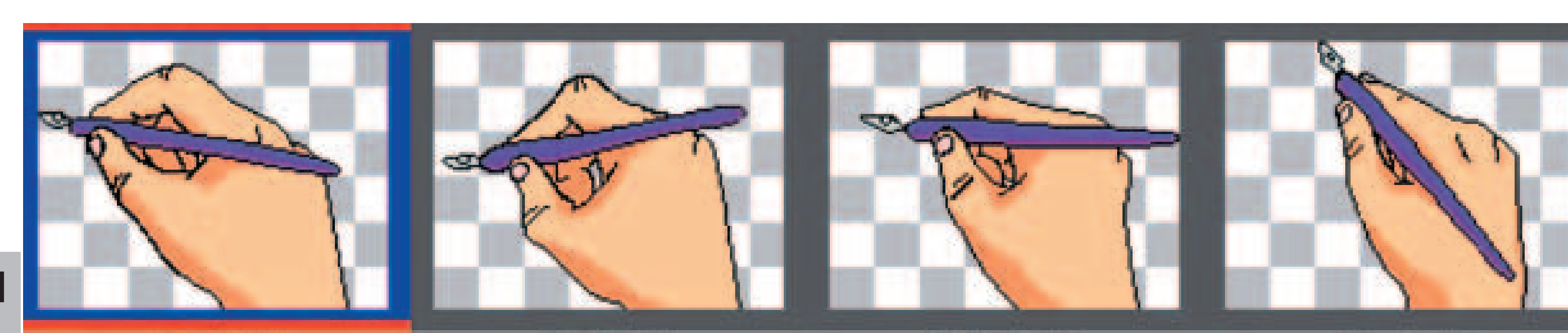
Jasc Animation Shop

Фирма Jasc позиционирует свой Animation Shop как GIF-аниматор. Но, честно сказать, выполняет он свои функции фуфлыжно. Зато возможность работы с другими форматами анимации в программе реализована просто великолепно. Ты можешь без проблем конвертировать любую анимацию в любой формат или сохранять свои творения в любом виде. Хотя бы только это может заставить тебя установить Jesc Animation Shop на свою тачку. Так что если тебе не жало потратить часик на выкачивание этой тулзы, то сделай это, в хозяйстве она пригодится.

<ИТОГО!?>

Как видишь, не существует определенной проги, которую можно было бы назвать лучшей для создания анимации. Каждая из них направлена на какую-то свою область. Где-то удобней создавать анимацию, а где-то управлять ею или оптимизировать размер результирующих файлов. Поэтому желательно держать несколько прог сразу на одном винте. Но самое главное - это выбрать для себя что-нибудь хорошо создающее анимацию и что-нибудь хорошо оптимизирующее. Что именно ты выберешь, зависит полностью от тебя, выбирать придется исходя из личных пристрастий и наклонностей.





PC_Zone

МЕНЮ-ГЕНЕРАТОРЫ

Horrific (smirnandr@mail.ru)

МЕНЮ-ГЕНЕРАТОРЫ

ОБЗОР ПРОГ ДЛЯ СОЗДАНИЯ МЕНЮ АВТОЗАГРУЗКИ НА ТВОИХ БОЛВАНКАХ

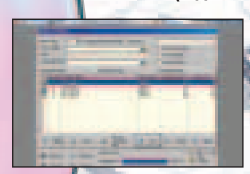
Мы уже делали обзор приводов CD-RW и описали необходимый для записи софт. Но тема записи болванок не может быть закрыта, пока мы не покажем тебе, какой существует софт для создания меню автозагрузки. Я понимаю, что ты не ламер и давно уже отключил автозапуск дисков в своих окошках. Но ведь твои корешки могли этого и не сделать. А как будет приятно их удивить прекрасной программой автостарта.

<EasySoft CD Menu-Generator>

http://www.easysoft.dk

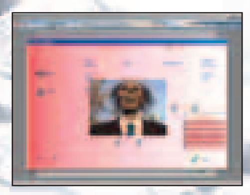
Тип: Shareware

Стоимость: $20 (с диском $28)



Окно проекта

Когда я впервые установил эту прогу, мне захотелось ее сразу стереть. Примитивное стартовое окно, и абсолютно нет никакого меню. Меня всегда пугали такие проги своей примитивностью и глупыми мастерами. Но почему-то я пересилил себя и создал новый проект (наверно, просто ради интереса). Буквально пять минут, и я уже не пожалел, что сделал это. Возможностей в программе куча, проблем еще больше :). Не, ну прога конечно отличная, просто дядя Билл в отношении таких тулз всегда говорит, что интерфейс интуитивно непонятен. Но это только на первый взгляд и только для интуитивно непонятливых перцев :). Лично я разобрался с работой тулзы где-то за пару недель :). Шутка, за день непосильного труда можно познакомиться с каждой загогулинкой утилы. Но, поверь мне, это того стоит.



Настройка визуального вида окна автостарта

Сразу после создания проекта перед тобой появляется окно, в котором можно настроить глобальные настройки. Среди них есть интуитивно непонятный параметр "Menu Type". Как ты думаешь, что это значит? Сразу говорю, что не угадал. Если ты там укажешь 1, то проги будут сжиматься с помощью архиватора RAR. Если там будет 2, то все зажмется в CAB архивы. Очень приятно, что прога умеет экономить место на болванке, но могли бы так и написать - "Выбор метода сжатия", потому что надпись "Menu Type" абсолютно тут не при чем. Помимо архивирования, отличительной особенностью проги можно назвать возможность защиты паролем. Это для тех, кто хочет продавать диски и защититься от пиратов. Но я думаю, что наших варезников средним пальцем не испугаешь.

<CDMenu Author>

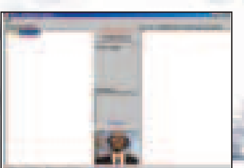
www.danbbs.dk/~duplex/

Тип: Пока был свободным



Главное окно

Сразу от сложного перейдем к простейшему. CDMenu Author - очень даже простая прога. Минимум настроек, не больше и возможностей. Зато с помощью этой утилы автораны создаются немного быстрее. Простота бьет и по интерфейсу. Ты не сможешь влиять на вид окна авторана, потому что все крепко прописано в программе и не поддается изменению. Единственное, что ты можешь указать, - заголовок окна и логотип, который показывается в центре окна. Минимум настроек бьет не только по визуальным возможностям создаваемых менюшек. Тулза не умеет автоматически архивировать, как это сделано в EasySoft CD Menu-Generator, поэтому придется все сжимать самостоятельно своими мозолистыми ручонками. Если ты хочешь в срочном порядке создать простой авторан, то лучше запустить эту прогу и не мучиться с другими. Лично я ее использую, когда хочу создать какой-нибудь диск с софтом своему корешу-ламеру.



Меню, созданное с помощью CDMenu Author

<Multimedia Builder>

www.mediachance.com

Тип: Shareware

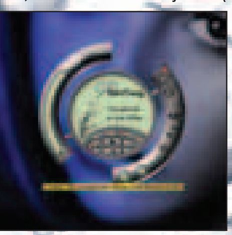
Стоимость: $45



Multimedia Builder

Эта тулза по возможностям, наверное, самая крутая. Но и повозиться с ней придется намного дольше. Прога из такого разряда, что по ней можно целые книги писать. Если ты знаком с векторной графикой, то многое из доступного в проге тебе будет понятно. Именно по принципу векторной графики ты рисуешь свои окна, кнопки и любые другие элементы управления. Тебя пугает слово "рисуешь"? Меня тоже, потому что именно этого я делать не умею, ну что поделаешь, что мне на руки в детстве медведь наступил :). Видимо поэтому я ненавижу эту тулзу.

Моя ненависть не позволила мне выкинуть Multimedia Builder из обзора, потому что все, кто хоть немного умеет рисовать, полюбят эту прогу до глубины души. Благодаря тому, что окна рисуются, их форма может быть любая. Посмотри на скрин ниже, этот авторан я взял из примеров, поставляемых с тулзой (я же говорил, что я рисовать не умею, поэтому даже не пытался повторить что-то подобное). Красотища? Вот именно.



Даже такой интерфейс можно забодяжить в Multimedia Builder

Достоинств у программы очень много, но есть один недостаток, о котором я не могу не сказать. Прога глючная и иногда вылетает. Слава Биллу, что хоть все окна за собой не тянет в полный даун.

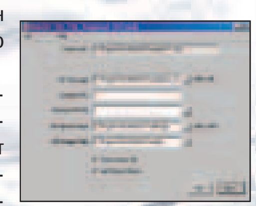
<MakeCD>

http://www.killersoftware.com/makecd.htm

Тип: Shareware

Стоимость: 24,95

И еще одна простая утилита. Все создание делится на два шага. На первом ты выбираешь имя проекта, картинку фона и картинку заголовка. На втором заполняются пункты твоего будущего меню авторана. Количество пунктов ограничено, и можно создать только 4 ссылки. Если тебе нужно быстро создать авторан и достаточно 4 ссылок, то лучше выбрать MakeCD. Полученный авторан страдает большим грузом лишних файлов. Окно будет строго квадратного размера, и никаких защит файлов и автоматических архиваций. Минимум возможностей говорит сам за себя.



Элементарно! Проверяем все пути и давим на пимпу

<Delphi или CBuilder>

www.borland.com

Тип: Коммерческая тулза

Стоимость: Очень дорого :) и зависит от жадности продавца.

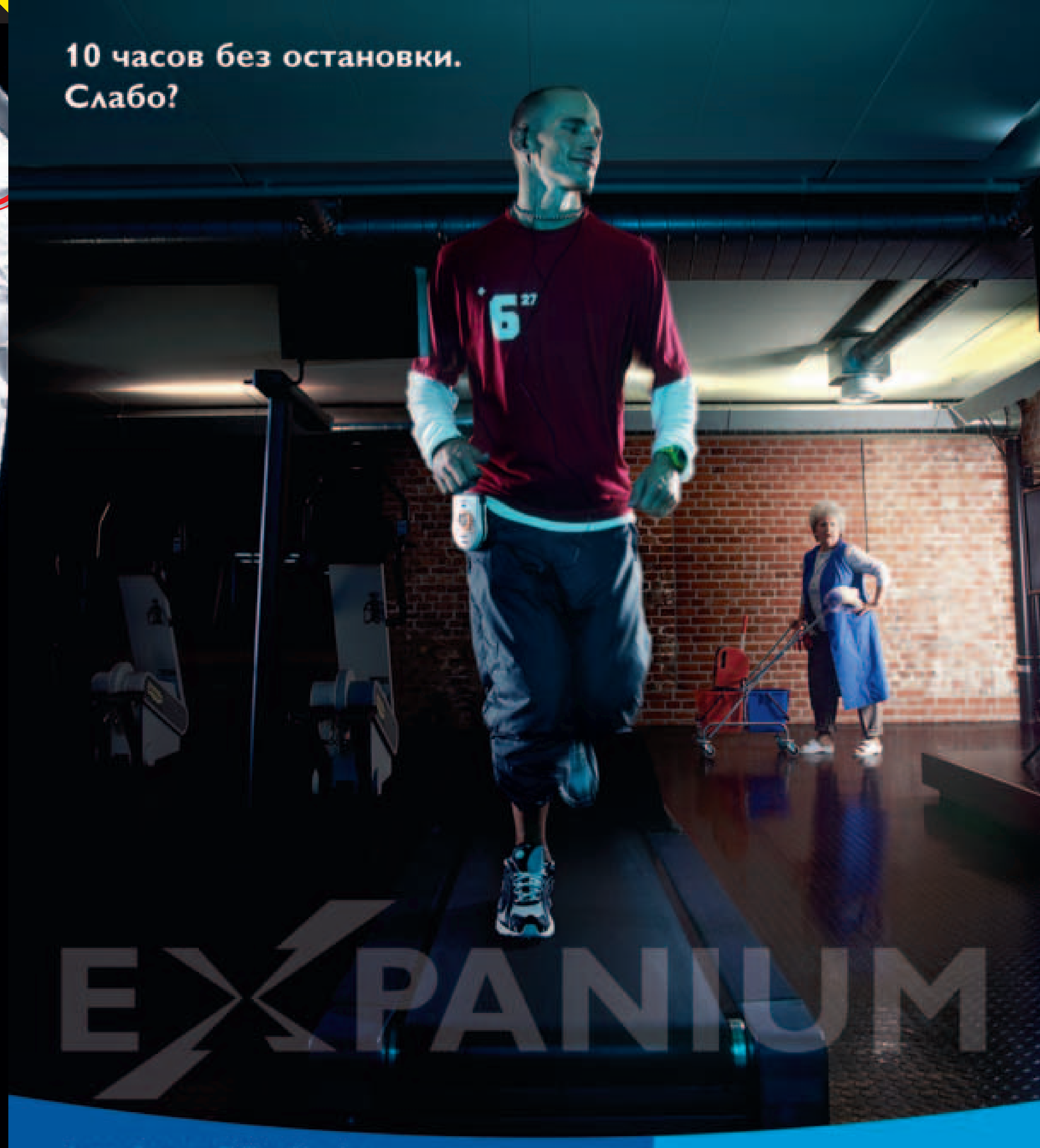
Не пугайся этой проги. В][уже давно существует рубрика Кодинг, и ты должен уже знать основы. Написать оболочку для твоей болванки на Delphi отнимет времени чуть больше, чем в любой специализированной проге, зато ты абсолютно ничем не ограничен. Все зависит от твоего полета мысли и заточенности рук. Я специально в заголовке привел сразу две среды разработки (Delphi и CBuilder), потому что обе они обладают великолепными визуальными возможностями и в то же время не ограничивают твой полет мысли. Разница только в том, на каком языке ты пишешь - паскаль или C++.

У меня на полке лежит коллекция из 300 дисков разных варезников, и в большинстве из них оболочка явно написана на одном из этих языков программирования. Почему? Да потому, что только если ты сам будешь кодить, можно создать менюшку, на 100% отличающуюся от других. Ну а самое главное - ты можешь со спокойной душой поставить на нее copyright и хвастать перед друзьями, что это создал именно ты.

<Disconnect>

На этом обзор я считаю законченным. Что именно выбрать - решать тебе. Если у тебя нет проблем с художеством, то выбирай Multimedia Builder. Если ты хоть немного разобрался в кодинге, то твой выбор - Delphi или CBuilder. Если нужна скорость, то это CDMenu Author или MakeCD. Ну а если ты хочешь получить что-то среднее между качеством и простотой, то однозначный выбор - EasySoft CD Menu-Generator. В любом случае, я советую тебе всегда держать под рукой или CDMenu Author, или MakeCD. Потому что иногда бывает очень нужно создать что-нибудь очень быстро, и качество не имеет особого значения.




10 часов без остановки.
Слабо?
6 27
eXPANIUM

PC_Zone

РУСИФИКАЦИЯ СВОИМИ РУКАМИ

 Shadow Bat (bat@bladezone.ru)

РУСИФИКАЦИЯ СВОИМИ РУКАМИ

КАК СДЕЛАТЬ ПЕРЕВОД ИНОЯЗЫЧНОЙ ПРОГРАММЫ

Хотелось бы тебе покопаться в интересной программе? Выяснить, как она выглядит изнутри, выдрать из нее красивые значки и картинки или вообще изменить ее внутренний интерфейс? Но для полноценной работы нужны исходники, нужно знать основы программирования… Вообще, нужно изучать очень много вещей, на которые совершенно нет времени. К тому же 80% разработчиков не подозревают о существовании «великого и могучего», а от английского интерфейса начинает тошнить… Есть довольно простой способ изменить если не принципы работы программы, но уж ее внешний вид точно.

<Пролог>

В феврале 2000 года из X я узнал о существовании программы Restorator. Хотя нет, скачал я ее еще пару месяцев назад, но не врубился, что она делает. На сайте автора было написано про exciting world of UCA's - User-styled Custom Applications, но это ничего не объясняло. А маленький абзац в X все прояснил - это программа для переделки других программ. На самом деле все довольно просто. В любой программе есть место, где в довольно упорядоченном виде хранятся почти все данные ее внешнего вида. И эти данные можно легко изменить, не обладая никакими основами программирования и не имея исходных кодов. Программы, которые могут изменять эти данные, относятся к классу редакторов ресурсов. За прошедшие полтора года этот класс довольно сильно разросся на волне популярности Restorator-а, появился даже один отечественный представитель.

<Теория>

Для начала немного теории, а потом я опишу известные мне редакторы ресурсов. Ресурсы чаще всего находятся в exe файлах, реже в dll, а вообще их можно найти везде - вплоть до файлов с экранными заставками (scr). Почти независимо от того, в чем сделана интересующая нас программа, они разделены по разным разделам/папкам. Все примеры я будут давать на базе программы Restorator, она обладает почти самым большим количеством возможностей и довольно проста в освоении.

Скачиваем, запускаем и видим три окна - «resource tree» - в нем показывается открытый файл со всем его ресурсами в виде раскрывающихся папок; внизу висит содержимое рабочей папки, куда будут извлекаться ресурсы и откуда они будут добавляться. Справа есть окно resource viewer, где будет отображаться содержимое открытого ресурса. В качестве примера возьмем всем известный блокнот, надеюсь, он у тебя есть. Открываем в ресторaторе notepad.exe - и что мы видим? А видим мы несколько папок - Menu, Dialog, String, Accelerators, Icon, Version. Некоторым людям, всю жизнь не вылезающим из танка, эти названия ничего не говорят, но нам-то ясно, что в папке Menu находятся стандартные меню, в папке Dialog содержаться окна диалогов. В папке String находятся текстовые отрезки, вставляемые в разные места программы, в Accelerators находится список сочетаний кнопок, который проставляется в меню. Так, что там еще осталось? Папка Icon содержит значки, а Version - информацию о версии программы. Так как блокнот не слишком продвинутая программа, в ней отсутствуют разделы с картинками - Bitmap, с видео - AVI, с функциями - Typelib. В программах, написанных на Delphi, есть еще раздел RCData. Некоторые типы данных - Menu, Dialog, String, Accelerators и RCData - можно редактировать во встроенном редакторе. Почти все типы данных, кроме version, можно извлечь и редактировать в других программах. А потом вставить обратно. То есть можно изменить все картинки программы, все видеовставки. Например, в Windows вместо перелетающего листочка можно поставить летающий кирпич, если у тебя настолько прямые руки, что могут редактировать видео. Все видеофайлы хранятся в формате Avi, а картинки чаще всего в Bmp, 256 цветов. Курсоры, иконки - все можно заменить. Нельзя изменить только информацию о версии программы, которая содержится в разделе Version. По мнению автора программы - изменение данных о версии может внести путаницу. Во время редактирования меню и диалогов все изменения автоматически будут отображаться в окне предварительного просмотра, что существенно облегчает задачу. Внизу каждого изменяемого файла будет несколько закомментированных строк. В нем довольно подробно, но по-английски, будет написано, что можно сделать с данным кодом. Теоретически, осмыслив эти комментарии, можно разобраться во всем, не читая данную статью.

<Проблемы>

Любое дело, кроме самого примитивного, содержит большую кучу проблем. И здесь нас не минует сия чаша.

Проблема номер 1:
Тип RCData содержит в себе одновременно и текст, и всю графику данного окна. С ним неудобно работать, серия Виндов 9x не может отобразить для редактирования очень большие куски текста. Попробуй, например, открыть в блокноте файл размером в мегабайт. Облом, да? И встроенный редактор Restorator-а также обломает. Конечно, можно все это извлечь, получив кучу рисунков и один txt файл. Но не факт, что это все запихнется обратно. Самым лучшим выходом является переход на Win NT/2K/XP, если ты этого еще не сделал.

Проблема номер 2:
Часто разработчики, наплодив громадных размеров исполняемый файл или озабоченные неприкосновенностью своего детища, сжимают его до совершенно непотребных размеров. Например, небезызвестный Winboost обладает exe файлом весом в 7 метров. После сжатия он уменьшается в 10 раз, вот только редактировать ресурсы в нем нельзя. При открытии таких файлов Restorator выдает надпись о поврежденных ресурсах. Эта проблема отчасти разрешима, причем в два этапа. Этап первый - находим программы для анализа файлов и выясняем, чем они сжаты. Этап второй - находим, чем файлы можно разжать, и разжимаем. Облом может наступить на любом этапе - или что-то не анализируется, или не разжимается, или разжатое не работает. Не работать может по двум причинам - либо сжимали по максимуму и ничего восстановить нельзя, либо разжатый файл поврежден. Тогда можно сделать такой финт ушами - загрузить в каком-нибудь редакторе ресурсов и сохранить. Очень помогает в таком случае Alchemy CATALYST.

Проблема номер 3:
В исполняемом файле нет никаких ресурсов или там какая-то фигня. Где тогда искать? Можно открывать по очереди все самые большие файлы в папке с программой. Можно посмотреть, что во время установки программы устанавливалось в системные папки windows. Можно посмотреть, к каким файлам обращается программа во время запуска. Можно «програбить» всю папку с программой на наличие текстовых ресурсов, а потом поискать в результатах какую-нибудь сложную фразу из программы и выяснить, откуда она выдрана.

Проблема номер 4:
Программа проверяет свою идентичность во время запуска. Тут надо искать кряк, который снимает эту защиту, или сделать его самому.

<А как сразу получить результат?>

Специально для тех, кто испугался всех трудностей и хочет получить результат, ни фига не делая. К счастью, в Рунете еще полно ненормальных, типа меня, которые готовы бесплатно поделиться результатами своих трудов. Допустим, позарез захотелось увидеть программу XXX на русском языке. Как можно изменить ее интерфейс? Вариантов целых три:

Если разработчики программы XXX умные предусмотрительные люди, они подозревают о наличии в мире других языков. Они делают в своей программе возможность смены языков. Чаще всего все данные о новом языке интерфейса содержатся в специальном файле, который я называю «языковой модуль». Надо разыскать в сети такой файл на нужном языке и подсунуть его программе. Чаще всего он подходит к разным версиям программы.

Если возможности легально изменить язык интерфейса нет, придется воспользоваться специальными патчами, которые заменят часть ресурсов программы на немного измененные. Название этих патчей - русификаторы. (К сожалению, у этого слова есть еще несколько значений, так что не запутайтесь.)

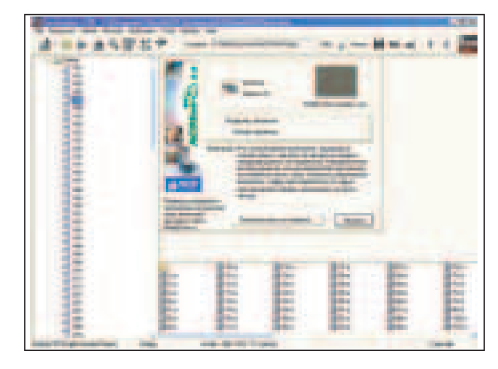
Третий вариант экзотический, для настоящих извращенцев. В мире существует уникальная программа, которая может «на лету» заменять английский интерфейс на русский. Называется это убожество LingoWare. Работает оно по словарю, который существует пока только для одной программы - ICQ. Это настоящий монстр. Требует денег, обладает жутким интерфейсом с поддержкой скинов, отжирает кучу памяти и заметно тормозит работу компьютера.

<Вооружаемся>

Теперь, когда все ламеры, испуганные теорией и проблемами, сбежали, начинаем вооружаться. Первым делом идут программы для изменения ресурсов.

Restorator

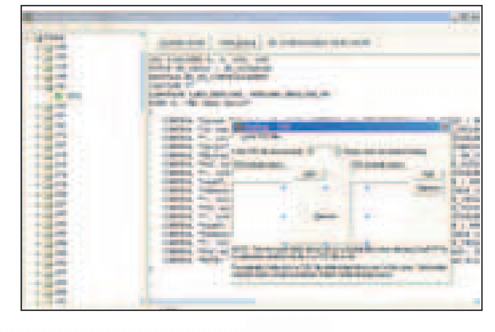
Самая известная программа. Обладает довольно понятным интерфейсом. Довольно подробное описание работы, справка и комментарии. Очень много интересной информации есть на сайте. Может "грабить" файлы и папки на наличие ресурсов. Зарегистрированная версия может создавать патчи, то есть автономные программы, которые будут вносить все изменения в ресурсы, которые ты сделал. Может отобразить почти все виды ресурсов. Из недостатков - небольшая глючность. Иногда виснет. Иногда отрубаются сочетания кнопок. Не идеальный поиск (в результате указывается только ресурс, содержащий результат). Медленно выходят новые версии. Нет визуального редактирования диалогов. Небольшой прикольный баг: предыдущая версия (2.50) могла зарегистрироваться без ввода регистрационного кода.



Ресторируем

Resource Hacker

Очень неплохая программа. Идеально дополняет ресторатор. Быстрая. Интерфейс простой. Нормальный поиск. Может редактировать HEX.



Resource Hacker все на свете перекорежит

Passolo

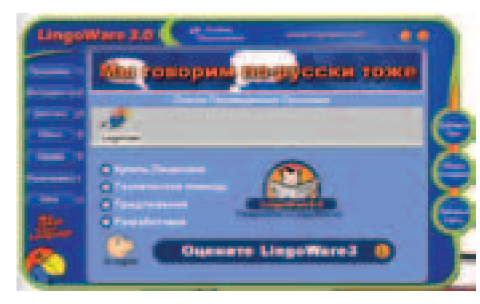
Для оперирования с файлами использует проекты, где записано, какие файлы, ресурсы и установки использовать с данной программой. Можно создавать словари с переводами слов, которые будут подставляться автоматически. Перед редактированием создается список текстовых фраз, который потом надо изменять. Но обычный тип, через дерево ресурсов все же есть.

Visual Localize

Программа похожа на Passolo, только более неудобный, но оригинальный интерфейс. Тоже используются проекты, тоже есть словари, так же создается список текстовых надписей. Большим плюсом является мощная система замены по шаблону и навороченная система просмотра. Без регистрации не дает изменять весь файл.

Alchemy CATALYST

Довольно продвинутая программа. Визуальный редактор. Подсчет букв в изменяемом сочетании. Редактирование ведется в двойном окне, где сразу показывается измененный вариант и оригинал. Без регистрации дает изменить только 10% от файла.



Алхимик-Катализатор

Resource Tuner

Обладает интерфейсом в стиле XP и прикольной текстовой строкой. Подключаются плагины. Без регистрации работает 30 дней.

ExeScope

Раньше это была довольно неплохая программа, но всеми ее достоинствами обладает Resource Hacker, а глюков у нее куча.

Есть еще старые и малоэффективные программы от крупных фирм. Например, Resource Workshop от Borland и ResourceStudio от Symantec.

Программы для анализа сжатых файлов. Так как это программы из арсенала хакеров, найти их в сети иногда довольно сложно. Почти все они заброшены довольно давно и не обновляются.

PE-Sniffer

Единственная Win программа. Анализирует файлы на наличие признаков самых распространенных программ для сжатия/защиты. Может определить компилятор.

File Analyzer, File Information, File Scanner

Все они работают из-под DOS. Выводят кучу информации, среди которой может быть то, что нам нужно.

Программы для разжатия. Если ты определил, чем была сжата нужная вам программа, следует воспользоваться программой для разжатия именно этой версии этого сжимальщика. Лучше подобрать коллекцию побольше, на всякий случай.

ProcDump

Самая известная и глобальная программа. Анализатор и распаковщик, поддерживает кучу форматов, может пересобрать исполняемый файл. Единственная программа, у которой есть win интерфейс.

UN-PACK

Аанализатор и распаковщик. Поддерживает плагины. В качестве плагинов использует File Analyzer, EXESCAN, DISASM, IDArc.

UnASPack - для ASPack, Ashell.

CASPR - для ASPack и ASProtect.

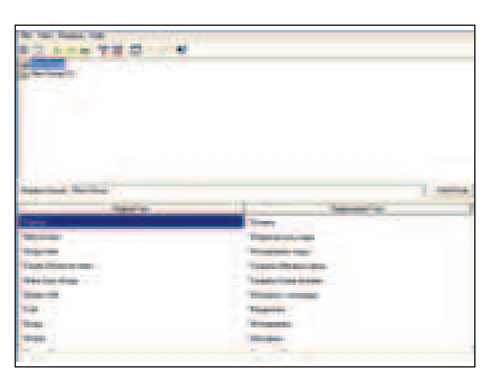
DeShrink - для Shrinker.

rAD - для r!sc's Asprotect.

Теперь переходим к программам, помогающим в быту.

Aditor Pro

Многооконный текстовый редактор. Подсветка синтаксиса. Режим замены. Возможность поиска в файлах. Довольно быстро открывает большие текстовые файлы. Идеальный редактор для извлеченных ресурсов.



BK ReplaceEm за работой

BK ReplaceEm

Программа для пакетного изменения текста в файлах. Вводите текст для поиска, текст для замены, указываете папку, и все ее содержимое меняется. Самое главное, что варианты поиска и замены можно сохранить. Таким образом, составив своеобразный словарь с самыми частыми словами, можно заменить половину извлеченных ресурсов.

Еще тебе понадобится Фотошоп или другой мощный редактор графики, HEX редактор, программа для просмотра графики, типа ACDSee, переводчик для перевода больших кусков текста.

Русификатор это:

1. **Специальный драйвер для ДОСа, заставляющий принтер нормально печатать русские буквы.**
2. **Специальная программа для КПК, позволяющая работать с русскими буквами.**
3. **То, про что написана эта статья.**



PC_Zone

РУСИФИКАЦИЯ СВОИМИ РУКАМИ

Shadow Bat (bat@bladezone.ru)

Сайты:

BladeZone.ru -
http://www.bladezone.ru

Nord Hacker's page -
http://www.rus.agava.ru

НПП Ноотехника -
http://www.noo.com.by/redactor.html

MSI Lab -
http://msilab.narod.ru/

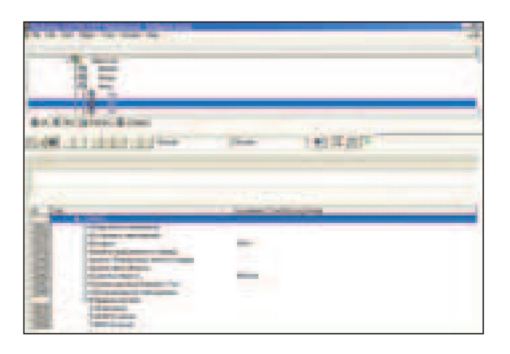
Russian R o w -
http://rusrow.boom.ru/

ukrUA.com.ua -
http://www.ukrua.com.ua/

cULt -
http://cultypa.boom.ru/

m0nkrus -
http://www.monk.al.ru/

ExE Tools (анализаторы и распаковщики) -
http://www.exetools.agava.ru/



Какая мощь!

<Практика>

Переходим к самому главному - редактированию меню и диалогов. Возвращаемся к открытому в Restorator-е блокноту. Раскрываем там раздел меню и видим ресурс под названием «1». Если его выделить, то в окне просмотра будет большая колонка очень знакомого текста. Если поднапрячь мозги и воображение, то можно сообразить, что это содержимое всех меню блокнота, за исключением контекстного. Переключаемся в режим редактирования (Viewer -> Edit Mode), это проще сделать нажатием на кнопку, обозначенную как «ab|». Теперь в колонку добавятся скрытые ранее символы, и ее можно будет редактировать. Выглядеть это будет так:

```
1 MENU
{
 POPUP "&Файл"
 {
 MENUITEM "&Создать\tCtrl+N", 1
 MENUITEM "&Открыть...\tCtrl+O", 2
 MENUITEM "&Сохранить\tCtrl+S", 3
 MENUITEM "Сохранить &Как...", 4
 MENUITEM SEPARATOR
 MENUITEM "Параметры страницы...", 5
 MENUITEM "&Печать...\tCtrl+P", 6
 MENUITEM SEPARATOR
 MENUITEM "В&ыход", 7
 }
 POPUP "&Правка"
 {
```

Теперь небольшое пояснение, что же это такое. Специально для тех, кто в жизни не видел листинг кода.
{ и } - Этими значками отмечается начало и конец меню.
& - Так отмечается подчеркнутая буква. Если при активном меню нажать с клавиатуры ту букву, которая подчеркнута в команде меню, эта команда исполнится. Знак ставится перед нужной буквой. Выбирать надо самые подходящие буквы. Повторять буквы нельзя, иначе фича не сработает - будет вызываться первая команда.
MENUITEM - название типа объекта. Иногда, в диалогах, имеет смысл поменять, чтобы все вместилось.
"чего-нибудь" - Изменять нужно именно то, что в скобках. Везде.
, 4 - Номер команды.
\tCtrl+N - Сочетание кнопок клавиатуры, вызывающее эту команду. Иногда все это прописано в отдельном разделе Accelerators.
Меню обычно самая простая часть программы. Там очень удобно все изменять. Во-первых - сразу виден результат. Во-вторых - нет ограничений по длине. Конечно, можно сделать команду из 96 символов, из-за которой все меню расползется на пол-экрана. Так что одно из основных правил - «краткость - сестра таланта». А в-третьих, не надо думать, что значит данная команда в данном контексте.
Диалоги. Это самая интересная и сложная часть. В блокноте наибольшим количеством признаков полноценного диалога обладает ресурс номер 12. Вот он какой:

```
12 DIALOG 0, 0, 356, 196
STYLE DS_SETFONT | DS_MODALFRAME | DS_3DLOOK | DS_CONTEXTHELP | WS_POPUPWINDOW | WS_VISIBLE | WS_DLGFRAME
CAPTION "Параметры страницы"
FONT 8, "MS Shell Dlg"
{
 GROUPBOX "Бумага", 1073, 8, 8, 224, 56, WS_GROUP
 LTEXT "Ра&змер:", 1089, 16, 24, 34, 8
 COMBOBOX 1137, 51, 23, 173, 160, CBS_DROPDOWNLIST | CBS_SORT | WS_VSCROLL | WS_GROUP
 LTEXT "Пода&ча:", 1090, 16, 45, 34, 8
 COMBOBOX 1138, 51, 42, 173, 160, CBS_DROPDOWNLIST | CBS_SORT | WS_VSCROLL | WS_GROUP
  GROUPBOX "Ориентация", 1072, 8, 69, 69, 56, WS_GROUP
 AUTORADIOBUTTON "&Книжная", 1056, 16, 82, 52, 12, WS_GROUP
 AUTORADIOBUTTON "&Альбомная", 1057, 16, 103, 52, 12, NOT WS_TABSTOP
 GROUPBOX "Поля", 1075, 85, 69, 147, 56, WS_GROUP
 LTEXT "&Левое:", 1102, 93, 85, 32, 8
 EDITTEXT 1155, 126, 82, 28, 12, WS_GROUP
 LTEXT "&Правое:", 1103, 163, 85, 32, 8
 EDITTEXT 1157, 196, 82, 28, 12, WS_GROUP
 LTEXT "&Верхнее:", 1104, 93, 104, 32, 8
 EDITTEXT 1156, 126, 103, 28, 12, WS_GROUP
 LTEXT "&Нижнее:", 1105, 163, 104, 32, 8
 EDITTEXT 1158, 196, 103, 28, 12, WS_GROUP
 LTEXT "В&ерхний колонтитул:", 32, 8, 135, 75, 8
 EDITTEXT 30, 85, 134, 147, 12, ES_AUTOHSCROLL
 LTEXT "Н&ижний колонтитул:", 33, 8, 154, 75, 8
 EDITTEXT 31, 85, 153, 147, 12, ES_AUTOHSCROLL
 DEFPUSHBUTTON "OK", 1, 184, 174, 52, 14, WS_GROUP
 PUSHBUTTON "Отмена", 2, 240, 174, 52, 14
 PUSHBUTTON "Прин&тер...", 1026, 296, 174, 52, 14
 GROUPBOX "Просмотр", -1, 240, 8, 108, 158
 CONTROL "", 1080, "STATIC", SS_WHITERECT, 254, 46, 80, 80
 CONTROL "", 1081, "STATIC", SS_GRAYRECT, 334, 50, 4, 80
 CONTROL "", 1082, "STATIC", SS_GRAYRECT, 262, 122, 80, 4
}
```

Первая строка содержит информацию о номере и размере данного окна. Первые две цифры равны нулю, так как это длина отступа от верхнего и правого края. 356 - это длина, а 196 - высота окна. Следующие две строки содержат описание стиля окна. Если тебе сильно не нравится/нравится что-то во внешнем виде, то это можно осторожно изменить без ущерба для работы. Полный список всех команд стиля данного объекта находится в комментариях внизу ресурса. Ниже написан заголовок окна и еще ниже тип и размер шрифта. COMBOBOX, CONTROL, LTEXT, EDITTEXT и т.д. - это разные контроллеры, переключатели, списки и весь остальной мусор, из которого состоит окно диалога. Иногда для экономии места имеет смысл аккуратно изменить тип, например, RADIOBUTTON на COMBOBOX. Не забывай про значок &. Про размеры объектов - они тоже состоят из четырех цифр через запятую; если их пять, то первая - номер этого объекта. Все эти размеры можно изменить. Если текст не влезает, а его размер увеличить нельзя, то можно сделать перенос на следующую строку с помощью кода \n. Правда, для некоторых объектов это невозможно. Если после переноса нижнюю часть не видно, увеличь высоту объекта.

Проверяй все измененные окна в разных разрешениях, с разным размером букв. Та надпись, которая нормально выглядит на 1024x768x96dpi, будет заметно кастрирована на 800x600x120dpi. А лучше заранее оставлять запас длины. Никогда не переводи надпись на буквах «ОК» как «Да». «Да» - это «Yes». А сочетание ОК настолько интернационально, что переводить его не надо. Меня, да не только меня, это бесит. Если ты уменьшаешь длину ниспадающего списка, всегда проверяй потом, чтобы слово, которое туда подставляется, влезло.

Следующим номером нашей программы идут стринги. Это такие специальные строчки, которые вставляются в сообщения об ошибках, в списки, во всплывающие подсказки. Самая большая сложность их перевода - правильно угадать, что значит переводимое слово там, куда оно вставится. У них нет никаких настроек, на них действуют настройки того, куда они вставятся. Вместо %% вставляется что-то определенное - имя файла, фрагмент текста из другого места, определенная дата или цифры.

```
STRINGTABLE
{
1, "Не удается открыть файл %%.\n\nПроверьте наличие диска в устройстве."
3, "Не удается найти файл %%.\n\nСоздать новый файл с таким именем?"
5, "Файл %% уже существует.\n\nЗаменить его?"
10, "Текст в файле %% был изменен.\n\nСохранить изменения?"
```



```
11, "Безымянный"
12, " - Блокнот"
}
И последним номером идет RCDATA.
object FormMain: TFormMain
 Left = 128
 Top = 62
 HorzScrollBar.Visible = False
 VertScrollBar.Visible = False
 ActiveControl = ChkBoxAutorun
 BorderIcons = []
 BorderStyle = bsNone
 Caption = 'WinBoost 2001 Gold Edition'
 ClientHeight = 453
 ClientWidth = 613
 Color = 8568008
 Font.Charset = DEFAULT_CHARSET
 Font.Color = 3355443
 Font.Height = -9
 Font.Name = 'MS Sans Serif'
 Font.Style = []
 Icon.Data = {

000001000100202000000000000000A80800001600000028
000000200000004000
 }
 OldCreateOrder = True
 Position = poScreenCenter
 Scaled = False
 OnCloseQuery = FormCloseQuery
 OnCreate = FormCreate
 OnShow = FormShow
 PixelsPerInch = 96
 TextHeight = 13
 object CoolForm1: TCoolForm
  left = 0
  top = 0
  width = 613
  height = 453
  Align = alClient
  Picture.Data = {

07544269746D617028B80C00424D28B80C00000000003
6000000280000006502
   }
OnMouseMove = SemuaMouseMove
  Mask2 = {00000000}
 end
```

То, что в виде цифр, - это рисунок и значок в виде двоичного кода. При извлечении становятся обычными файлами. Здесь частично действуют правила диалогов, например, стили и размер объекта. Только записаны они в другом виде. Раздел RCDATA бывает только в программах, сделанных на Дельфи. Сюда навалено в одну кучу все подряд - текст, рисунки, звук, видео, меню. Для русификации надо изменять Caption = 'XXXX' и Hint = 'XXXX'. Иногда ресурсы RCDATA записаны в виде HEX кода.

<Результат>

После того, как переведены все меню, диалоги, стринги и перерисованы надписи на рисунках, русификация в принципе готова. Осталось создать результат, то есть патч, который будет заменять все измененные вами ресурсы у других. Патч можно сделать и в Restorator-е, и в сторонних программах. Допустим, у тебя есть в одной папке оригинальный файл notepad.exe и измененный файл notepad1.exe. Открываем в Restorator-е измененный файл, запускаем мастер создания патчей (Tools-> Create ResPatcher...) Next, вводим имя оригинального файла notepad.exe. Дальше вводим имя файла, который получится после запуска патча, всякие инструкции и свои координаты. В патч войдут все измененные в Restorator-е ресурсы (они отмечены стрелочками). Кстати, сам патч тоже сжат, так что просто так ресурсы, которые в нем содержатся, из него не достанешь.

<Как все удачно пропатчить>

Патч перед заменой ресурсов сравнивает размер файла с тем, на основе которого его делали. Если размер не совпадает, то облом. После замены ресурсов файл записывается поверх старого, а старый сохраняется как backup (если не снята отметка в патче). Так что если во время замены ресурсов данная программа открыта или файл «только для чтения», то тоже облом.

<Проблема с русскими буквами>

Иногда после установки какого-нибудь русификатора вместо русских букв получаются крокозябры. Тогда нужно внести небольшое изменение в реестре:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Nls\CodePage\
Соответствие кодовых страниц 1250, 1251, 1252 и 1253 надо установить файлу c_1251.nls (для Win 95/98/ME) или cp_1251.nls (для Win NT/2000/XP)

<История в вебе>

И в самом конце немного истории про bladezone.ru и про русификаторщиков. Август далекого 1999 года. Мне стукает в голову мысль создать сайт нашего квейк-клана. Буквально через несколько дней на чат.ру появляется новая пага в темно-темно красных цветах. Почти сразу, через месяц, до нас доходит, что мы как клан никого не интересуем. Рождается новая идея - создать сайт, посвященный всему тому, что нам нравится. Костяк клана - Shadow Bat, L'Mago и DeXTeR - собираются и решают, что там будет. А будет описание софта, игр на PC и консолях и юмор. Каждому по разделу. Пага разрастается. Ее новое имя Center BLADE. Примерно в начале 2000 года рождается 2 новых раздела - описание книг и русификаторы. Идея создавать русификаторы приходит в голову мне, то есть Бату. Вся ее простота показывается Декстеру на моментальном переводе программы Cheat'O'Matic (одно окно, 2 кнопки). Титаническим усилием Бат переводит программу ZipMagic, а Декстер - Microangelo 98. Всеобщее ликование. Данным патчам придумано название - русификаторы. Описание этих русификаторов помещается на новый софтовый сайт - HotSoftZone (с автором которого я довольно быстро подружился). Это дело становится известным. Примерно месяц мы доказываем всем, что наши русификаторы - это не вирусы и не трояны и что, устанавливая их, ты не портишь свой компьютер. Делаются два громадных перевода - я перевожу часть интерфейса Windows 2000 pro, а Декстер - ICQ 99. Уже март 2000 года. Находится еще один русификаторщик - это Nord Nacker с сайтом www.rus.agava.ru. Мы тоже перебираемся на агаву. HotSoftZone становится Softarea.ru, а наши русификаторы висят там как самые скачиваемые программы. Мы уже хотим зарабатывать на сайте, а агава со своими баннерами нам мешает и часто глючит. Покупается платный хостинг и адрес blade.net.ru. Делается несколько очень сложных переводов - Flash 5, FrontPage 2000, Dreamweaver. Наши русификаторы появляются на пиратских дисках. Я пытаюсь связаться с авторами самых крупных программ и выяснить, не можем ли что-нибудь получить за их перевод. Выясняется, что все, что они могут предложить, - это крупный штраф или судебное разбирательство. Общее мнение такое - мы не рассчитываем выходить со своими продуктами на российский рынок, где все воруют, и не хотим, чтобы вы лазили грязными руками в наши детища и повышали их популярность в вашем регионе. Наступает наше время. Мы уже обзавелись адресом bladezone.ru, переведено примерно 40 разных программ. Русификаторы становятся популярными, по запросу русификатор Windows XP с Яндекса приходит по 200 человек в день, что составляет 10% посетителей. Мы находим единственный способ заработка с нашего дела - продажа болванок с записанными русификаторами. Появляется все больше сайтов с русификаторами. Каждый пятый сайт на народе «про варез» содержит раздел "русификаторы", в котором находятся содранные наши переводы и переводы NH. На данный момент в сети примерно 5 сайтов реальных русификаторщиков, еще 5 недоступны или не обновляются. Под новый 2002 год листовый счетчик натикал 2 лимона хинтов. И как апофеоз - Х предлагает мне про это все написать. Вот это, блин, призвание...

Программы:

- **Restorator - http://www.bome.com/Restorator/**
- **Resource Hacker - http://rpi.net.au/~ajohnson/resourcehacker**
- **Passolo - http://www.passolo.com/**
- **Visual Localize - http://www.vizloc.com/**
- **Alchemy CATALYST - http://www.alchemysoftware.ie**
- **Resource Tuner - http://www.heaventools.com/**
- **ExeScope - http://www.vector.co.jp/authors/VA003525/**
- **ProcDump - http://ProcDump32.cjb.net**
- **UN-PACK - http://unpack.cjb.net**
- **Aditor Pro - http://aditor.swrus.com/**
- **BK ReplaceEm - http://www.orbit.org/replace/**

P.S. Несколько советов тем, кто будет использовать это как руководство к действию:

1. Если ты всерьез решил заняться переводом, старайся делать это тщательно и без ошибок, особенно орфографических. Не уподобляйся нашим замечательным пиратам.

2. Не пытайся «доделывать» чужой перевод. Особенно без спросу. Программ хватит всем, а автор может обидеться.

3. Не используй русификаторы для пакостей. Ну или не распространяй их как русификаторы. Очень просто создать патч, который будет тайком менять местами кнопки «Форматировать» и «Закрыть». И очень сложно потом доказать, что не все русификаторы в рунете делают это.

4. Если ты переводишь программу, делай это до конца.



PC_Zone

НАУЧИ СВОЙ ЛЮБИМЫЙ СОФТ УВАЖАТЬ РУССКИЙ ЯЗЫК

Horrific aka Фленов Михаил smirnandr@mail.ru
http://www.cydsoft.com/vr-online/.

НАУЧИ СВОЙ ЛЮБИМЫЙ СОФТ УВАЖАТЬ РУССКИЙ ЯЗЫК!

Полный мануал по русификации программ продвинутыми хакерами

Немного обидно становится, когда скачиваешь какую-то прогу, а она пишет тебе все диалоги, менюшки и сообщения на буржуйском языке. А когда пытаешься залезть в языковые настройки, то обнаруживаешь, что можно установить десяток разных языков, кроме родного русского. Такое ощущение, что нас с тобой не уважают :). Мы уже столько лет в Инете, а буржуи до сих пор не научились разговаривать на русском языке:). Непорядок!!! Если больших корпорашек мы смогли научить уважать русского брата, и они выпускают локализованные версии своих прог, то вот с шароварщиками такая песня не проходит. Они продолжают делать только англоязычные версии своих шедевров. Оно и понятно, ведь только с буржуев можно снимать зеленые. Наш брат лучше найдет кряк, чем отслюнявит свои кровные за какую-то прогу :).

<ЧТО И ЧЕМ ЛОКАЛИЗОВЫВАТЬ>

Ну, ничего. Сегодня мы научим этот программный сброд уважать русский язык. Сразу предупрежу, что описываемые сегодня мной методы могут сработать с большинством прог, но не со всеми. Абсолютно все проги невозможно подогнать под одну гребенку и научиться их локализовывать. Тут все зависит от кодера, написавшего прогу, а они любят извращаться по делу и без. Лучше всего к локализации приспособлены проги, написанные на Visual C++ с каким-нибудь визуальным интерфейсом. Просто все, что создается в Visual C++ визуально, сохраняется в виде ресурсов и пришпандоливается к запускному файлу практически в чистом виде. Эти ресурсы потом можно без проблем вытаскивать, редактировать и запихивать обратно. Ну что поделаешь, что дядя Билл даже ресурсы не смог защитить. Ну хоть бы какую-нибудь примитивную защиту поставил.

В Инете достаточно много прог для редактирования этих ресурсов. Все они работают приблизительно одинаково, поэтому какую выберешь ты, это зависит от тебя. Наиболее предпочтительными, на мой взгляд, являются Restorator и Resource Workshop. Первая из них имеет больше возможностей и позволяет редактировать ресурсы прог, написанных не только на Visual C++, но и на Delphi. Вторая предназначена только для ресурсов из Visual C++, но более удобная и более продвинутая. Я решил показать тебе Resource Workshop - просто потому, что я его больше люблю.

Мою любимую Resource Workshop можно найти на любом диске с полным вариантом Delphi. Программа ставится очень примитивно и не задает лишних вопросов. В качестве главного ее достоинства я бы назвал возможность редактирования ресурсов не только в текстовом виде, но и в визуальном. Это значит, что тебе не нужны глубокие познания в том, как устроены ресурсы программ и что там можно изменять. Все действия выполняются щелчками мыши и легкими ударами по клаве. Поэтому мозги нам сегодня не понадобятся :). Можешь отложить их на полочку и поберечь до лучших времен :).
Ну ладно разговоров, пора что-нибудь русифицировать.

<НА СТАРТ!!!>

Давай выберем какую-нибудь прогу и русифицируем ее. Я для примера взял W32Dasm - мой любимый дизассемблер. Русификацию нужно начинать с запускного файла. Именно в нем всегда находится наибольшее количество ресурсов, которые нужно подправить. Итак, запускаем Resource Workshop. Перед тобой открывается простецкое окно с двумя пунктами меню (как видишь, все очень просто, и мозги тут не нужны :)). Но это только пока, сейчас оно изменится. Выбери в меню File->Open, и перед тобой откроется окно открытия файла. Оно немного непривычное, но, с другой стороны, достаточно удобное.

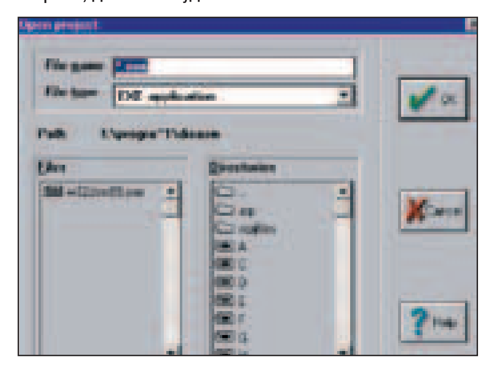


Рисунок 1. Окно открытия файла

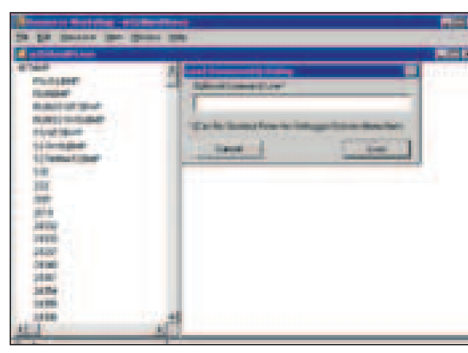


Рисунок 2. Resource Workshop с открытым файлом

Для начала в выпадающем списке File Type выбери тип "EXE Application", чтобы ты мог открывать запускные файлы. Теперь найди нужный запускной файл и открой его. У меня это W32dsm89.exe. Вот теперь в твоем окне появилось намного больше менюшек и куча всяких возможностей. На рисунке ты можешь увидеть Workshop в действии.

Как видишь, все окно вертикально разбито на две части. Слева перечислены все доступные в файле ресурсы. Любой из них ты можешь выделить и сразу визуально увидеть его в правой части окна.

<ТИПЫ РЕСУРСОВ>

Все ресурсы разбиты по разделам. Нас будут интересовать следующие разделы:
1. Bitmap - картинки. Здесь могут быть спрятаны простые рисунки, высвечивающиеся в окнах диалогов.
2. Menu - меню, они и в Африке меню.
3. DIALOG - здесь находятся различные окна диалогов.
4. STRINGTABLE - таблицы строк. В этих таблицах могут быть любые сообщения, выскакивающие в строках состояния или в простых окнах.
5. ACCELERATORS - здесь спрятаны сочетания клавиш быстрого вызова каких-нибудь команд.
6. CURSOR - курсоры, они и в Африке курсоры.
7. ICON - я думаю, что это понятно.
8. VERSIONINFO - информация о версии. Тут ничего особенного нет, поэтому здесь творить нечего.

Если ты тоже решишь русифицировать W32Dasm, то заметишь, что в нем есть все из этих типов ресурсов. Поэтому я выбрал именно эту прогу.
Внутри разделов находятся сами ресурсы, которые могут называться по-разному, но в основном программеры ставят какие-нибудь числа. Просто программеры уже окончательно ушли внутрь компа и думают только числами. Нормальные слова им уже непонятны :). Тебя это не должно смущать, но и менять имена ресурсов на другие нежелательно.
Если тебя заинтересовал какой-нибудь ресурс, то просто щелкаешь по нему два раза и попадаешь в удивительный мир редактирования.

<РЕДАКТИРОВАНИЕ КАРТИНОК>

Самое простое - редактирование ресурсов из раздела BITMAP, т.е. картинок. Для примера щелкни дважды по ресурсу 333 в разделе BITMAP, и ты попадешь в простой графический редактор.



Рисунок 3. Редактирование картинки

Когда будешь редактировать картинку, не вздумай изменять ее параметры. В некоторых случаях это может пройти незаметно, а иногда может повлиять на стабильность проги. Так что если захочешь полностью заменить картинку, то делай ее такого же размера.
И еще, картинки в ресурсах не могут иметь глубину больше 8 бит. Это значит, что ты не сможешь разгуляться в цветовой палитре, потому что она ограничена 256 цветами.

<РЕДАКТИРОВАНИЕ МЕНЮ>

При русификации картинки не играют особой роли, потому что там текста практически не бывает. С рисунками ты можешь просто поиздеваться, чтобы приукрасить прогу и сделать ее более прикольной. Зато менюшка - это главное, с чего начинается любая локализация.

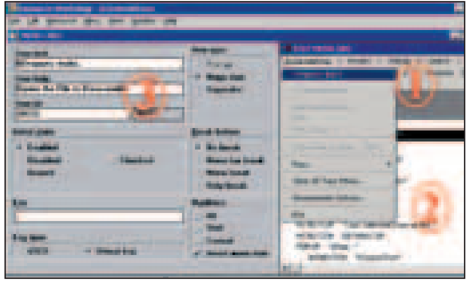


Рисунок 4. Окно редактирования менюшки

Давай дважды щелкнем по имени ресурса менюшки (номер 203) и попадем в соответствующий редактор. На рисунке 4 ты можешь увидеть его окно. Оно разбито на 3 части:
1. Справа вверху находится визуальная менюшка.
2. Справа внизу находится то же самое, только в виде текста.
3. Слева находятся свойства выделенного пункта меню.
Для выделения подлежащего редактированию элемента ты можешь пользоваться как визуальным меню (справа сверху), так и текстовым. Просто выделяешь нужный и изменяешь свойства.
Какие свойства надо менять? Первым делом нужно отредактировать "Item Text". Это текст, который будет отображаться в менюшке. Можешь еще подправить "Item Help" - текст подсказки, появляющийся в строке состояния. Остальное лучше не изменять.

<РЕДАКТИРУЕМ ДИАЛОГИ>

Следующим этапом в локализации всегда идет редактирование диалогов. Дважды щелкни по любому диалогу, и ты попадешь в визуальный редактор, отдаленно напоминающий Delphi.
Здесь ты можешь добавлять новые элементы типа картинок и текста для украшения твоего любимца различными прибамбасами. Сами же прибамбасы находятся в маленьком окошке "Tools" справа. Удалять что-нибудь не рекомендуется, потому что, как всегда, хочется удалить именно то, что может повлиять на работу проги.

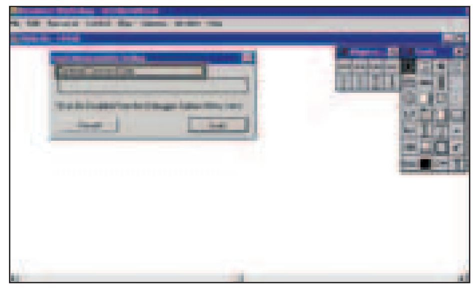


Рисунок 5. Окно редактирования диалогов

Для редактирования уже существующего текста нужно просто дважды щелкнуть по нему, и перед тобой появится окно для редактирования свойств текста (рисунок 6). Здесь тебе нужно подправить заголовок "Caption", чтобы надпись засияла русскими буквами.

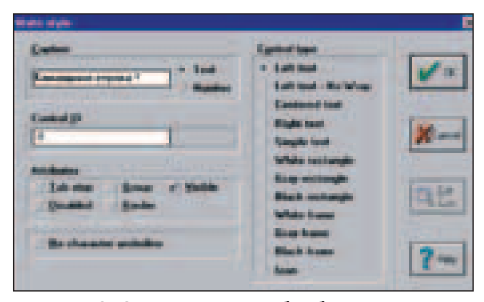


Рисунок 6. Окно свойств прибамбаса

Если у надписи есть какие-нибудь непонятные знаки типа звездочек, черточек или еще чего на первый взгляд ненужное, то не торопись удалять. Некоторые чудо-программеры, когда не хватает мозгов, начинают совать какие-нибудь знаки, которые потом меняются во время исполнения на что-нибудь другое. Если ты удалишь эти знаки, то прога может не заработать.

<РЕДАКТИРУЕМ ТАБЛИЦЫ СТРОК >

Ну и последнее, что должен русифицировать любой локализатор - таблицы строки. Это простые списки строк, в которых хранятся различные сообщения.
Давай дважды щелкнем по любой строчке в разделе STRINGTABLE. Перед тобой откроется окно, как на рисунке 7. Как видишь, здесь есть таблица, состоящая из трех колонок:

1. ID Source
2. ID Value
3. String

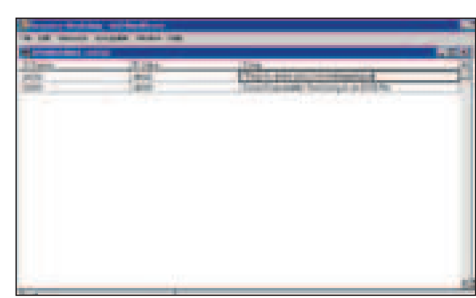


Рисунок 7. Редактор таблицы строк

Первые две колонки - это номера сообщений, и их менять нельзя. Тебя в основном интересует третья колонка, в которой хранится сам текст сообщения. Просто щелкай крысой в нужной строке и переводи ее на русский язык.

<СОХРАНЯЕМ РЕЗУЛЬТАТ >

Прежде чем сохранять результат, лучше сделать резервную копию на случай наличия драйвера КривыеРуки.sys. Этот драйвер может случайно сработать у тебя, но чаще всего срабатывает у программера, который что-то перемудрил при загрузке ресурсов.
Резервная копия нужна и в том случае, если программа категорически не хочет воспринимать русский язык и показывает вместо нормального текста разные закорючки. В этом случае у тебя есть два выхода:
1. Попробовать изменить в наглую тип шрифта. Вот это уже удобнее делать с помощью программы Restorator.
2. В худшем случае можно вернуться обратно к английскому языку.
С помощью Resource Workshop тоже можно попытаться заставить прогу уважать Россию. Для этого нужно выбрать из меню File->Preferences и в появившемся окне установить в поле Language for Win32 русский язык. После этого щелкаешь по нужному ресурсу правой кнопкой мыши и в появившемся меню выбираешь пункт "Language".

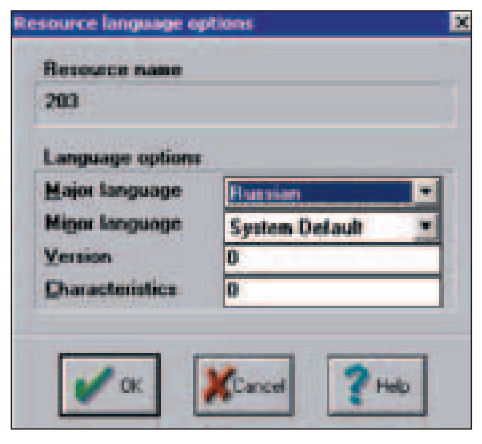


Рисунок 8. Изменение языка ресурса

<ЧТО ЕЩЕ? >

После того как ты русифицируешь запускные файлы, можешь приняться за динамические библиотеки dll. В них тоже могут быть ресурсы, которые нужно русифицировать. Открою секрет, некоторые dll могут содержать вообще только одни ресурсы. Поэтому тут всегда можно разгуляться.
Редактирование динамически загружаемых библиотек ничем не отличается от запускных файлов, поэтому сам разберешься.
Если ты не смог русифицировать свою любимую прогу, а она поддерживает несколько языков кроме русского, то не отчаивайся. Попробуй просмотреть все файлы, входящие в состав проги. Особенно посмотри наличие директории Language. Вот, например, в знаменитейшей проге Windows Commander есть такая дира. В ней лежат простые текстовые файлы, в которых находятся все строки и сообщения для Windows Commander. Просто переводи их и используй без всяких дополнительных усилий.
Ну а если ты решил русифицировать игру, то тут уже мои методы не подходят. Там программистская мысль настолько извращена, что каких-то рекомендаций дать невозможно. В свое время я пытался заниматься этим делом, но в играх нет определенных правил. Поэтому каждую игру приходится штудировать по косточкам. Но это уже совершенно другая история.

<НАПУТСТВИЕ>

На этом я хочу распрощаться. Если есть вопросы, пиши. Только сразу напоминаю, что мой способ русификации работает не всегда, но очень часто. Так что вопросы типа: "Почему я не могу русифицировать XXX прогу" - не принимаются. Возможно, она написана без использования ресурсов, поэтому у тебя и ничего не выходит. И еще. С помощью редактирования ресурсов можно не только русифицировать, но и издеваться над программами. Ты можешь вставлять в диалоги собственные фотки, изменять любые картинки, рисуя факи, маки и другую мазу. Ну и, конечно же, можно изуродовать программу по своему усмотрению до неузнаваемости.

PC_Zone

ХАКЕРЫ ВЫБИРАЮТ CVS

 Ovod (ovod@crazy.ru)



Хакеры выбирают CVS

Система контроля версий CVS

Часто случается так, что в разработке проекта участвует более одного программиста, и еще чаще все разработчики раскиданы по стране, а то и всему миру. Каким образом они будут работать над файлами так, чтобы изменения, сделанные одним разработчиком, были доступны другим? Ты можешь возразить, сказав, что после работы над файлом его можно закачать на фтп сервер так, чтобы другие разработчики имели к нему доступ. Но представь, что будет, если над одним файлом работает одновременно два человека, изменения, сделанные одним, безвозвратно будут утеряны. Именно в таких ситуациях приходят на помощь системы контроля версий - control version system.

В их обязанности входит контроль сделанных изменений. При желании можно просмотреть, кто и что где изменил. Также каждому файлу присваивается версия, при желании можно вернуться к более ранней версии, если внесенные изменения были неправильные: например, разрабатываемая программа перестала функционировать после чьих-то изменений.

На данный момент существует несколько систем контроля версий: CVS от сообщества Open Source и Visual Source Safe от Microsoft. Если разрабатывается программа, скажем, на Visual Basic, то это не означает, что ты должен использовать Source Safe, так как объектом этих систем могут быть практически любые файлы. В рамках этой статьи мы рассмотрим именно CVS, так как она абсолютно бесплатна и доступна для свободного скачивания в отличие от продуктов Microsoft.

Программа CVS является идеальным средством для разработки программного обеспечения на базе как Интернета, так и локальных сетей. Это приложение типа «клиент-сервер», в котором сеть используется в качестве транспортного уровня, а сам сервер - центральный банк исходных текстов. Внутри банка данных отдельные проекты объединяются в модули. Когда разработчик внес все необходимые изменения, он помещает измененный файл в банк данных. Остальное программа CVS берет на себя. CVS необычайно широко применяется при разработке подавляющего большинства современных проектов с открытым исходным текстом. Среди огромного списка операционных систем и программ (FreeBSD, XEmacs, XFree86, OpenSSL) выделяется, пожалуй, лишь ядро Linux, главный разработчик которой, Линус Торвальдс, в силу особенностей личности отказывается использовать какую бы то ни было систему управления версиями, кроме собственного мозга. Да и почти все остальные участники разработки держат свой собственный CVS-репозиторий, которым активно пользуются при разработке. Проект sourceforge.net, обеспечивающий свободно доступную инфраструктуру для разработчиков свободного программного обеспечения, в качестве стандартной возможности предоставляет использование своего CVS-сервера. Вообще, количество инсталляций и пользователей - одно из значительных преимуществ CVS.



Официальный сайт CVS

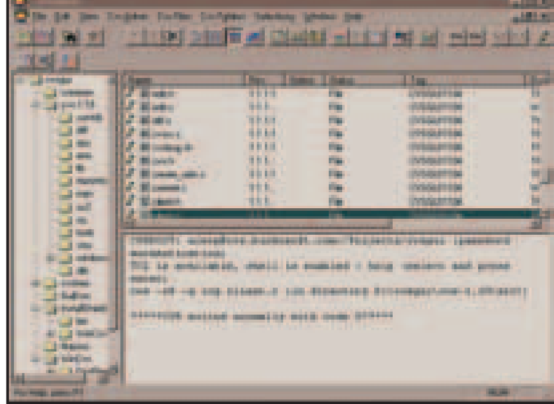
<Основные команды>

cvs login - входит на сервер CVS. Для успешной регистрации этой команде нужен пароль.
cvs checkout <имя модуля> - позволяет получить модуль из банка данных.
cvs update <имя файла> - обновляет локальную копию файла.
cvs commit <имя файла/каталога> - передает локальную версию файлов или каталогов на сервер CVS.
cvs add <имя файла/каталога> - добавляет новый файл или папку на сервере CVS. cvs remove <имя файла/каталога> - удаляет файл или папку с сервера CVS. На самом деле данная команда не удаляет файл, у тебя сохранится доступ к предыдущим версиям.
cvs status <имя файла> - показывает состояние модификации локальной версии файла.
cvs diff <имя файла> - показывает различия между двумя версиями файла. По умолчанию выводятся различия между локальной и удаленной версиями.

<Пример сеанса работы>

Допустим, у нас есть два разработчика: Вася и Петя, которые работают над проектом гостевой книги. Также предположим, что руководитель проекта установил сервер CVS, создал в банке данных модуль с именем GuestBook и соответствующим образом установил значения настроек программы CVS. Сначала разработчики должны «захватить» копию модуля GuestBook с сервера, для этого используется команда cvs checkout, которая создает локальную папку с названием, совпадающим с именем модуля.

```
vasya@dev:mnt/daten/home/vasya > cvs login
CVS password: <password>
vasya@dev:/home/vasya > cvs checkout guestbook
cvs server: Updating guestbook
U guestbook/messages.pl
U guestbook/signup.pl
```



WinCVS

Теперь у обоих разработчиков есть локальная копия модуля, можно приступать к работе. Заранее Вася и Петя договорились, что один будет работать над файлом messages.pl, выводящим сообщения в гостевой книге, а другой - над signup.pl, необходимым для добавления сообщения в гостевую книгу. Прими во внимание, что CVS не может заменить общение между членами команды! После того как Вася закончил свою часть работы, он собирается вернуть файл в центральный банк данных. Поскольку кроме него этот файл никто не редактировал, можно ограничиться одной командой:

```
vasya@dev:/home/vasya/guestbook > cvs commit messages.pl
```

Теперь система запустит стандартный текстовой редактор (для Unix это чаще vi, а для Windows это notepad) и запросит сообщение, которое будет связано с данной версией файла. Это сообщение могут видеть другие разработчики, поэтому оно должно точно описывать внесенные изменения. Иногда команды разработчиков используют даже эти сообщения для автоматической передачи заказчику подробного отчета о проделанной работе. В любой момент можно запросить состояние файла с помощью команды:

```
vasya@dev:/home/vasya/guestbook > cvs status messages.pl
```

Результат данной команды показывает, что локальная копия файла messages.pl - самая свежая. В системе также предусмотрены следующие обозначения: Up-to-date - локальная копия идентична копии на сервере CVS. Locally Modified - локальная копия была изменена и еще не принята сервером. Locally Added - файл только что был добавлен в локальную папку. Locally Removed - файл только что был удален из локальной папки. Needs Checkout or Needs Patch - версия в удаленном банке данных более новая, чем локальная, которую нужно обновить. Needs Merge - версия в удаленном банке данных более новая, чем локальная копия, которая была модифицирована. Это приведет к слиянию версий при обновлении. Unknown - файл не находится под контролем системы CVS.

Каждой новой версии, освобожденной разработчиком и зарегистрированной в банке данных, автоматически приписывается номер. Это позволяет получить произвольную версию файла. С помощью команды cvs diff разработчик может просматривать списки различий между какими-либо версиями, не имея соответствующих файлов.

<WinCVS>

Программа WinCVS представляет собой графический клиент для системы CVS. В данный момент он может функционировать не только на Windows, но и даже на Apple. Зная вышеописанные обозначения, ты с легкостью сможешь разобраться с этой не трудной, но очень полезной программой. Приятно, что она сделана очень грамотно и обладает интуитивно понятным интерфейсом.
За рамками статьи остались такие обширные темы, как администрирование системы CVS, маркеры и ветви, автоматизированные уведомления и т.д. Я рассмотрел только клиентскую часть, но не стоит недооценивать полезность CVS. Ведь если ты являешься любителем Open Source продукта, то CVS тебе будет очень кстати. Все самое свежее можно скачать именно с CVS серверов. Поэтому не останавливай свои мозги - изучай новое :).



Полезные ссылки

http://www.cvshome.org - официальный сайт системы CVS, на нем можно найти полную документацию на английском. А в разделе download и сам сервер CVS.

http://www.wincvs.com - здесь можно скачать графический клиент для системы CVS. Клиент многоплатформенный, поддерживает Windows, Apple и т.д.

http://alexm.here.ru/cvs-ru/ - переводы различных документаций по CVS.

http://www.cvsnt.org - сервер CVS для Win32

Взлом

МАССИВНЫЙ IRC FLOOD

CuTTer (cutter@real.xakep.ru)

МАССИВНЫЙ IRC FLOOD

ФЛУД-АТАКИ НА КАНАЛАХ

< Folder 1 >

У тебя, вероятно, не раз возникало желание зайти на канал человека, однажды тебя обидевшего, и начать там гадить, поливать нечистотами, в общем - самовыражаться :). Возможно, ты сделаешь и захват канала, что тоже похвально. А вот я предлагаю привести ботов 100-200 на канал и заставить каждого говорить. Представляешь, что будет? Некоторые dialup'щики изза забитого канала просто вылетят из Инета. Но обо всем поподробнее.

БОЛЬШАЯ МЕСТЬ

Не будем вдаваться в подробности, отчего у тебя может возникнуть желание пофлудить на IRC каналах, а просто поговорим о том, как это реализуется. Сразу оговорюсь, писать никаких программ не придется, уже все написано. Хакер зарелизил свой собственный X-пакет утилит по irc flood'у. Он состоит из трех частей:

1. Обычный flood на канале. На канал забегает указанное число ботов, каждый бот произнесет любую фразу, например, "Мы полетим в космос". Потом боты убегают, и далее все начинается сначала. Так повторяется n-ое количество раз.

2. CTCP и флуд приватными сообщениями. Боты получают список пользователей с определенного канала и начинают флудить CTCP и приватными сообщениями. Также имеется friendlist - ники друзей, которым не стоит делать подобные гадости.
3. Интерактивный флуд-бот. Здесь самому решать, что флудить да как флудить. Просто вводятся IRC команды, а боты их исполняют. Суперская утилита :).

Скачать это добро можно с www.xakep.ru в разделе "Релизы журнала". Весь софт написан (пинайте, пинайте меня :)) на Perl. Выбор этого языка сделан по ряду причин. Во-первых, я хорошо знаю перл, а в нем очень удобно работать с сокетами, но самое главное: Perl установлен на всех хостингах под управлением *nix систем, и нет разницы, Linux это или FreeBSD. Насчет хостинга: работать скрипты будут именно оттуда. Объясняю, почему: если использовать данные утилиты локально, то при коннекте на IRC сервер у ботов будет только один хост, например, maravan.ru. А так как на всех серверах стоят ограничения на количество соединений с одного IP, то в итоге не выйдет большого флуда. В случае с хостингами получается, что в наличии находятся сотни адресов, но тут важен еще один момент. Очень вероятно, что все домены расположены на одном IP, т.е. есть два сайта www.care.ru и www.intimuslugi.ru, оба они ничем не связаны, но если ввести команду ping или nslookup, то станет ясно, что за ними кроется один и тот же IP - 194.135.30.66. Такой хостинг не подойдет. Необходим другой, выделяющий для каждого сайта свой IP. Например: www.ariadnamedia.com, www.hostrocket.com, www.apollohosting.com, они под каждый сайт дают новый айпишник. И самое последнее: очень важно наличие telnet или ssh доступа, без него невозможно узнать о состоянии работы флудботов.

ПРАКТИЧЕСКИЕ УПРАЖНЕНИЯ :)

Перед тем как запустить злобных ботов, их необходимо настроить. Настроек немного, но всех их придется произвести. Начнем с первого типа флудботов, которые просто засыпают множеством сообщений на канале. Они делятся на два вида: все ники генерируются случайным образом и являются незарегистрированными, второй - ники зарегистрированы, а сочетания nickname/passwords извлекаются из отдельного файла nicks.

Первая утилита называется channel.pl. Вот ее настройки:

```
$addr="irc.starlink.ru" - IRC сервер
$port=6667 - порт сервера

$num=1 - общее количество атак
$nummes=2 - количество атак на канале
$users=50 - количество ботов
$numsym=12 - размер ника ботов
$hosts='hosts' - имя файла с хостами

$info="bot" - информация, выдаваемая по whois
$nick="" - префикс в имени
$channel='#ruschannel' - атакуемый канал
$mes1='мараваны захватят мир!' - сообщение, которым будут флудить боты
$mes2='maravans's war' - сообщение при выходе с канала
```

А вот примерное содержание файла hosts:

```
konfetka.ru
nuclonstc.com
russianlaws.com
nac.ru
kortes.ru
welcom.ru
petexpress.ru
arsen.net
```

Чем больше доменов расположено на хостинге, тем лучше. Ведь каждый из них можно использовать при атаке. Вообще, список этих доменов можно получить разными путями. Например, если это хостинг, расположенный на площадке alabanza.com (www.ariadnamedia.com, www.apollohosting, www.cgi-bin.ru), то загляни в файл

/etc/hosts. В нем прописаны все возможные хосты. Еще некоторые хостинговые службы назначают системные имена пользователей, идентичные их доменам. Так что придется потратить время и составить список. Настроив и получив список доменов, запускай программу: ./channel.pl. На экране должна получаться примерно такая картина:



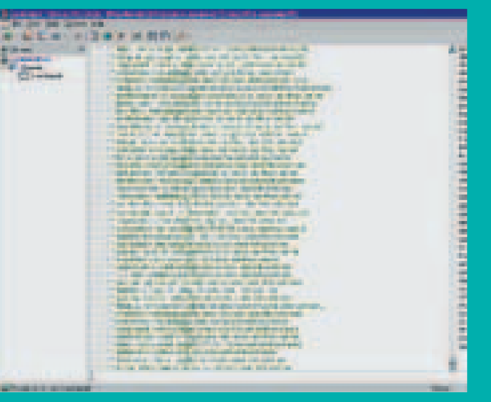
Боты собираются :)

После успешных соединений всех ботов к IRC серверу наступит самое интересное: хлынет шустрая толпа :). Боты начнут заходить на канал, писать сообщение на канал и быстро убегать. И так будет происходить указанное количество раз. Смотрится это просто суперски.

Правда, данную красоту можно очень просто пресечь. Если это IRC сервер с NickServ/Chanserv сервисами, то, установив флаг +R, ты можешь обломаться. Этот флаг разрешает заходить на канал только с зарегистрированными никами, а у нашего бота в данном случае ники таковыми не являются. Так что данный флубдот пролетает, но мы тоже не глупые. В комплекте наличествует скрипт channel-nick.pl, реализовывающий все то же самое, но использующий файл nicks, в котором расположена база с никами и паролями. Формат базы такой:

```
nick1:password1
nick2:password2
```

Правда, программа сама не регистрирует ники, они должны быть получены заранее. Поэтому придется попыхтеть, составить большую базу с нормальными регистрированными никами. Зато ключ +R теперь уже не остановит ботов.



Атака на канале

После жизнерадостных атак, наблюдаемых каждым посетителем канала, перейдем к более скрытным. В состав пакета входит программа private.pl. Она такая же в настройке, как и первая, но принцип работы другой. Поначалу боты собираются всей дружной толпой на сервере. После чего один из ботов заходит на атакуемый канал, получает список сидящих, уходит с него, и начинается flood. В чем он заключается? Теперь боты не забегают на канал, а начинают отсылать сообщение по приватам, далее делают разнообразные CTCP запросы, вроде: TIME, VERSION, PING. Однажды я попробовал это на себе, в итоге мой IRC клиент из-за множества открытых окон просто подвис :). Дабы такого не происходило с тобой и твоими друзьями, в программе есть friendlist. Он находится в конце программы:

```
push (@list, 'Gibbon', 'SideX', '_RS_', 'Deil', 'Ch1ck', 'Spider[]', 'CuTTer');
```

Это обычный массив с никами. Добавляй нужные имена, пускай программу (./private.pl) и наблюдай реакцию посетителей канала.

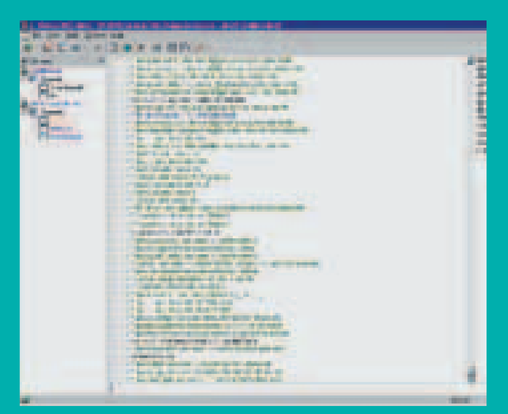
Чем хороши такие атаки: от них трудно защищаться, так как придется отключать разрешение на прием всех приватных сообщений. Также незаметно количество атакующих, ведь для получения списка сидящих "светится" всего один бот. Здесь не поможет и флаг +l, лимитирующий максимальное количество человек на канале. Это скорее всего вообще лучшая атака, если нет желания в открытую показывать всю свою мощь :).

Завершающей утилитой является интерактивный флудбот (программа intbot.pl). С ее помощью можно творить любые вещи, какие заблагорассудится. Допустим, зайти на кучу каналов, вести беседу одновременно сотнями ботами, потом перейти на другой канал поругаться к кому-нибудь в приват. Тут все зависит только от полета фантазии, я же расскажу только, как ее реализовать через ограничения intbot.pl.

В настройке самого скрипта нет необходимости, все значения программа спросит сама. Это адрес/порт сервера, количество ботов, какие ники использовать: случайные или зарегистрированные. Далее придется подождать некоторое время, пока все боты не соединятся с IRC сервером, после чего появится приглашение для ввода команд. Команды вводятся в соответствии с RFC1459. Вот краткий список:

JOIN #channel - зайти на канал #channel
PART #channel :message - покинуть #channel с сообщением message
PRIVMSG #channel :message - обычное сообщение на канале
PRIVMSG nickname :message - послать приватное сообщение человеку с ником nickname
NOTICE nickname :message - послать notice

Также я добавил свою команду JOKE. Она меняет всем ботам имена на новые случайные. JOKE может пригодиться, если вдруг всех ботов перебанили по никам, но надо отметить, что такое происходит редко. Теперь можно и экспериментировать :).



Реакция оперов

Вооружившись этими тремя утилитами, ты можешь дать достойный отпор противнику, но не стоит очень усердствовать. Если каждый начнет пользоваться этим только для самоутверждения своего "Я", то в IRC начнется хаос. А разрушать всегда проще, чем строить. Так что перед использованием подумай, чего ты хочешь добиться своими поступками.



Взлом

SHELLCODE СВОИМИ РУКАМИ

Buggzy (alienhard@mail.ru)



SHELLCODE своими руками

В этом тексте ты найдешь ответы на многие интересующие вопросы о переполнении буфера: что такое переполнение стека, как находить уязвимые программы, как писать эксплоиты, можно ли написать универсальный эксплоит, существует ли универсальная защита от переполнения стека и многое другое. В конце я дам некоторые приемы, интересные опытному юзеру.

< Folder 1 >

ЧТО ЭТО И КАК РАБОТАЕТ?

Допустим, в какой-то процедуре используется буфер для хранения данных и буфер находится в стеке. Под буфер выделен определенный объем памяти. Кроме того, есть еще несколько переменных, тоже хранящихся в стеке. Посмотрим, как все это выглядит.

```
<переменная 3 - 4 байта>
<переменная 2 - 4 байта>
<буфер - 1024 байта>
<переменная 1 - 4 байта>
<адрес возврата - 4 байта>
```

Мы наблюдаем в стеке три переменные и "адрес возврата" - 4-байтовое число, описывающее, куда передать управление после того, как текущая процедура доработает до конца. Теперь предположим, что программа хочет записать данные в N-ый байт буфера. Как она это сделает? К адресу начала буфера будет прибавлено N, и данные будут записаны по полученному адресу. Все правильно, но что будет, если N=1025?
Обычно компилятор не проверяет, чтобы N принимало допустимое значение, и оставляет это на совести человека. А что, если человек не подумал об этом? Тогда данные, которые должны были попасть в буфер, попадут в другую область памяти, что и называется переполнением буфера, а для случая, когда буфер лежит в стеке, - переполнением стека.
В нашем случае, при N=1025, они изменят значение <переменная 1>. При N=1029 изменится и значение адреса возврата, и после окончания работы процедуры управление будет передано не по тому адресу, по которому задумывал создатель, а по адресу, взятому из данных, переполнивших буфер. Если атакующий сознательно переполнил буфер, то он может подставить такой адрес, что будет выполнен любой код, какой он захочет.

Автоматический поиск переполнений

Скорее всего, возникают мысли по созданию утилиты, проверяющей любой стандартный сервис на наличие переполнений. Группа eeye (www.eeye.com) утверждает, что многие свои знаменитые баги в Microsoft IIS они нашли именно так.

ЗАЧЕМ НУЖНО ЭКСПЛУАТИРОВАТЬ ПЕРЕПОЛНЕНИЯ?

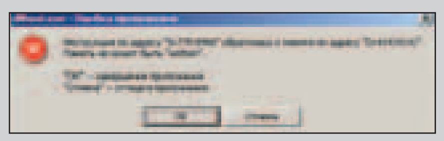
Код, выполняемый при переполнении, признается системой кодом той программы, в которой была уязвимость. Т.е. он выполняется на той машине, где находится уязвимая программа, и с правами, которые имеет эта программа. Таким образом, атакующий может повысить свои права доступа или получить управление над удаленной машиной.

КАК ИСКАТЬ ПЕРЕПОЛНЕНИЯ?

Самое примитивное переполнение буфера - работа со строками в текстовых протоколах (HTTP, SMTP, POP, FTP). Вот классический пример ошибки, найденной незадолго до написания статьи в одном из FTP-серверов "made in China" под управлением Windows. При подключении к серверу передается строка: "pass AAAAAAA...." - больше 1024 символов. Если в сервере нет переполнения, он должен сообщить об ошибке и работать нормально, а если есть - то он оборвет соединение и нередко вообще перестанет работать (ситуация, когда сервер перестает работать после определенным образом сконструированного запроса, называется DoS-атакой, но это не очень интересно). Другой способ поиска переполнений - анализ исходного кода или дизассемблирование программы - требует наличия исходника, бинарника, умения программировать и дизассемблировать, и поэтому многим не понравится. Однако многие уязвимости можно найти только таким способом.

КАК ПИСАТЬ ЭКСПЛОИТЫ?

В нашем примере сервер пытается записать наши "AAAA..." в буфер, но места там не хватает, и, как и описано, адрес возврата функции затирается значением 0x41414141, соответствующим четырем байтам 'A'. После завершения процедуры управление передается по этому адресу. Естественно, что там нет ничего интересного, и программа-сервер просто завершается с ошибкой General protection fault: "программа обратилась к адресу 0x41414141 и будет закрыта". А нам бы хотелось совершать более интересные действия. Вернемся к изображению стека и посмотрим, как нужно сконструировать данные.



Реакция на переполнение

■Итог - после переполнения буфера переменная 1 примет новое значение (что иногда помогает нам, иногда мешает, а иногда на это наплевать), а после выхода из процедуры начнут выполняться 1024 байта нашего кода, которые находятся сейчас в стеке. Эти 1024 байта могут, например, открыть порт 5000, ждать подключения к нему и запускать командный интерпретатор /bin/sh (для *никса) или cmd.exe (для NT, Win2K и XP), организовав некое подобие сервиса telnet. За любовь к вызову OS Shell этот тип кода называют shellcode, шеллкод.

СТЕК	ПЕРЕДАВАЕМЫЕ ДАННЫЕ
<буфер - 1024 байта>	<наш код - 1024 байта>
<переменная 1 - 4 байта>	<новое значение переменной 1>
<адрес возврата - 4 байта>	<адрес нашего кода в стеке>

СОЗДАНИЕ ШЕЛЛКОДА

Шеллкод - низкоуровневый код, специфичный для операционной системы. Вряд ли в рамках этой статьи удастся научить тебя низкоуровневому программированию под все ОС, так что придется понадеяться, что ты уже научился этому раннее. Здесь будут затронуты только специфичные для шеллкода проблемы.

1. Ограничение на набор символов.
Программа может считать шеллкод чем угодно, только не шеллкодом. Например, если программа работает с данными как со строкой символов (функциями strcpy и т.п.), то шеллкод не должен содержать символ с кодом 0, иначе часть шеллкода после этого символа будет проигнорирована. Возможны и другие ограничения на набор символов. Кроме того, программа может обрабатывать данные, заменяя один символ на другой - это тоже надо учитывать. Чтобы получить шеллкод без нулей, придется пофантазировать. Однако неправильно считать, что шеллкод никогда не может содержать символ с кодом 0 - все зависит от конкретной программы.

2. Мобильность кода.
При эксплуатации переполнения буфера не всегда известно, какой точный адрес будет у кода в памяти. Что делать, если нужно обращаться к данным, находящимся внутри шеллкода? Вот типичный способ определения адреса текущей инструкции:

```
call $+0
pop eax
```

В регистре eax окажется адрес инструкции, следующей за командой call. Однако команда call $+0 содержит "нехорошие" символы - два байта с кодом 0. Вот способ обхода.

```
jmp beforedata
afterjump:
pop eax

beforedata:
call afterjump
```

Команда pop eax приведет к тому, что в регистре eax окажется адрес, следующий за call, а там удобно разместить секцию данных.

3. Обращение к функциям системы.
В случае *никс-шеллкода все просто - обращение к функциям системы производится через int 80. А вот с windows дело обстоит хуже: через прерывания, оставшиеся в наследство от dos, ничего особо хорошего не сделаешь, максимум - записать что-нибудь в файл или запустить программу. Работа с более современными функциями - сеть, графика и т.п. - осуществляется через вызовы библиотек.
При загрузке программы сообщаются адреса всех нужных ей функций, а вот кто сообщит их шеллкоду? Если мы точно знаем, что по такому-то адресу в памяти находится обращение к такой-то функции библиотеки, то нам повезло, но эти адреса зависят от версии программы. Тут нам поможет поиск по сигнатуре: допустим, мы знаем, что кусок кода программы определенного вида содержит вызов нужной нам функции. Например, мы ищем кусок кода по шаблону FF 15 XX XX 40 00 A3 XX XX 40 00 и знаем, что в нашей программе это - вызов GetCommandLineA из kernel32.dll.
Другой способ - искать по сигнатуре саму библиотеку kernel32.dll - так делает, например, интернет-червь CodeRed. При этом мы может обратиться к области памяти, недоступной для чтения, и вызвать аварийное завершение программы. Для перехвата аварийного завершения нужно установить Structured Exception Handler, реализацию технологии смотри в самом CodeRed :).

НА ЧЕМ ПИСАТЬ ШЕЛЛКОД?

Шеллкод необходимо писать на ассемблере, но не обязательно, чтобы ассемблер был под ту же ОС (эксплоиты для linux вполне можно писать на tasm32), но важно, чтобы он был рассчитан на ту же архитектуру процессора. Для тех, кто ассемблер не любит, могу посоветовать утилиту от team teso, превращающую код на си в шеллкод без нолей. Но, честно говоря, человеку, не знающему ассемблер, пытаться создавать эксплоиты довольно сложно, и никакие утилиты тут не помогут :). Обычный прием - сделать бинарник, содержащий шеллкод, и вырезать его оттуда. Однако не пытайся вырезать куски "настоящих" бинарников - код, находящийся в них, в качестве шеллкода непригоден! Unix-бинарники обращаются к системным функциям через библиотеку libc, виндовские - через .dll-библиотеки, при этом код привязывается к таблице импортов бинарника, и работать отдельно от _своего_ бинарника не будет.

МИФ ОБ УНИВЕРСАЛЬНОЙ ЗАЩИТЕ

При переполнении стека выполняемый код также находится в стеке (а обычно при нормальной работе системы такого не бывает), и кому-то, по слухам, нашему соотечественнику Solar Designer'у, пришла в голову идея, что запрет исполнения кода, находящегося в стеке, позволит навсегда решить проблему переполнения стека. Используя хитрый трюк ушами с особенностями процессоров Intel 586 (именно 586, на 386 и 486 это не сработает, хотя кто о них сейчас помнит), ему удалось это реализовать в своем проекте OpenWall. Также существует патч для ядра Linux'a - PAX, заложенный во многие дистрибутивы, например, BlackCat, и коммерческий продукт под Windows - SecureStack, автор - другой наш соотечественник.
К несчастью (или к счастью?), это - далеко не выход. Ведь можно положить в стек данные таким образом, что после возврата из процедуры управление будет передано любой функции, принадлежащей основной программе, например, memcpy, и параметры ее вызова тоже будут находиться в стеке на положенных местах. В результате функция скопирует данные из стека в другую область памяти, где исполнение кода разрешено, а после возврата из нее управление будет передано в эту область памяти.

ЭКСПЛУАТАЦИЯ ПЕРЕПОЛНЕНИЯ "ВСЛЕПУЮ"

А что, если мы не знаем адрес возврата, длину буфера, расстояние от буфера до адреса возврата и вообще не видели уязвимую программу, а знаем лишь, что она находится на таком-то IP-адресе и таком-то порте? Возможно ли добиться выполнения шеллкода? Ответ - ДА! Некоторыми нетривиальными путями возможно добиться и этого.
Во-первых, нам нужно знать адрес буфера в памяти. Примерный адрес мы знаем - он чуть меньше, чем начальный адрес



Взлом

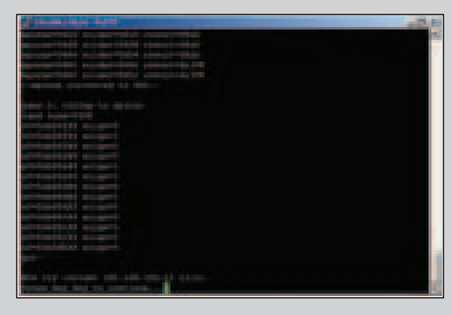
SHELLCODE СВОИМИ РУКАМИ

Buggzy (alienhard@mail.ru)

стека. Например, в linux он будет чуть меньше, чем 0xbfffffff. Насколько "чуть"? На сотню-тысячу байт. Сколько попыток нужно, чтобы угадать его? Нет, не сотня-тысяча. Нам не обязательно знать адрес шеллкода в памяти с точностью до одного байта, ничто не мешает нам разместить перед шеллкодом "посадочную зону" из большого количества NOP-ов, нам достаточно попасть адресом возврата в эту зону. Количество попыток перебора, таким образом, сведется к менее чем десяти. Во-вторых, нам нужно знать примерную длину буфера. Ее мы подберем методом "деления на два", или "недолет-перелет". Вот псевдоисходник программы, реализующей это:

```
mpzone=0;slider=0x1000;
do {
mpzone+=slider;
if(!try)mpzone-=slider;
slider=slider/2;
} while(slider!=0);
```

Функция try - псевдофункция, определяющая, был ли "недолет" или "перелет". В случае "недолета", т.е. допустимого размера данных, удаленная программа продолжает функционировать нормально, а в случае "перелета" - подвисает, обрывает соединение или совсем выпадает. Если выпадает совсем, реализовывать эту технологию долго - надо ждать, пока админ приведет сервис в работоспособное состояние. Работа алгоритма завершится на том, что будет найден максимальный размер данных, при котором удаленный сервис работает нормально. Эту область данных я буду называть MP-зона (от лат. monopenisuale). Для более корректного нахождения MP-зоны функция try должна проверять способность сервиса принять данные не один раз, а несколько, с различным значением данных. Такая проверка гарантирует, что внутрь MP-зоны можно помещать любые данные, и на работоспособность сервиса это не повлияет.



Поиск MP-зоны

Что такое MP-зона с точки зрения программы? Понятно, что MP-зона не меньше места, выделенного в стеке под буфер. Но она может быть и больше, вот картинка:

СТЕК	ПЕРЕДАВАЕМЫЕ ДАННЫЕ
<буфер - 1024 байта>	<MP-зона>
<переменная 1 - 4 байта>	<MP-зона>
<адрес возврата - 4 байта>	<новый адрес возврата>

Если значение переменной 1 не влияет на работоспособность программы, то она также попадает в MP-зону. Однако значение этой переменной может быть критично:

```
char *var1="correct";

recv(s,buff,5000,0); - получение данных
if(strcmp(buff,var1)==0) - сравнение буфера с
переменной 1.

return 0; возврат из процедуры
```

Ссылки по теме

Smashing The Stack for Fun and Profit (Aleph1)
http://www.phrack.com/show.php?p=49&a=14

eEye Digital Security
http://www.eeye.com/

Online shellcode generator
http://www.deepzone.org/olservices/xploitit

Team Teso Releases
http://www.team-teso.net/releases.php

В этом случае мы не можем присвоить переменной 1 произвольное значение - она является указателем на область памяти, содержащим строку "correct". Если после переполнения там окажется "левое" значение, то функция strcmp вызовет ошибку, и программа "вылетит", до исполнения нашего кода дело не дойдет.
Мы не можем точно знать, что находится после MP-зоны - одна из критичных переменных или адрес возврата, а нам нужно как-то перезаписать его. Вот два приема, позволяющие решить эту проблему.

1. Побайтовый подбор.
Размер данных увеличивается на 1, и последний байт подбирается так, чтобы сервис сохранял работоспособность. Способ хороший, почти универсальный, но далеко не всегда работает. Например, если наши данные обрабатываются как ASCIIZ-строка, то в конце данных обязан быть символ с кодом 0 - это не позволит нам подобрать последний символ, т.к. его значение нам неподвластно.

2. Наполнение достаточным числом адресов возврата.
Мы не будем пытаться определить, что находится после MP-зоны, а просто поставим в нее адрес возврата, повторенный достаточно много раз. Учитывая, что компиляторы выравнивают данные в стеке, все указатели, находящиеся между буфером и адресом возврата, будут указывать на один и тот же адрес, на него же будет указывать и адрес возврата. Способ тоже интересный, но если в ту область данных что-то запишут, то в момент возврата из процедуры там будет уже не шеллкод, а неизвестно что.

3. Этот способ - модификация второго.
После MP-зоны записываются убывающие значения, шаг убывания равен длине шеллкода. Это гарантирует нам, что указатель после переполнения будет указывать на область памяти, находящуюся после шеллкода, и одновременно избавляет нас от необходимости угадывать расстояние от MP-зоны до адреса возврата - любое из значений может подойти в качестве адреса возврата.
Все эти способы требует также знания еще одного параметра: "выравнивания". Нет гарантии, что разница между началом буфера и адресом возврата кратна четырем. Вообще, MP-зона вполне может "заезжать" в область критичных переменных, поэтому нам придется подбирать еще один параметр брутфорсом: на сколько байт необходимо сократить MP-зону. Для этого надо перебрать значения от ноля до трех.

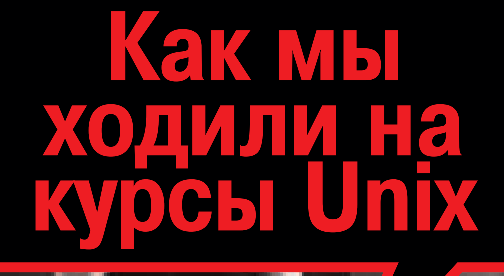
Итог - если пользоваться третьим способом определения значения критичных переменных, нам потребуется порядка 50 попыток, чтобы "вслепую" выполнить произвольный код даже в довольно тяжелых случаях, когда мы ничего не знаем о структуре стека уязвимой программы. За исключением зависимости от протокола, этот эксплоит, снабженный шеллкодами под все ОС, будет универсальным. Вот так мы достигли worldwide rulez'а...

Взлом

ХОЧУ ЗНАТЬ ЮНИКС!

CuTTer (cutter@real.xakep.ru)

Хочу знать Юникс!



< Folder 1 >

Актуальность UNIX систем возрастает с каждым днем. Подавляющее большинство серверов, подключенных к Интернет, работают под *nix системами: FreeBSD и Linux. Но Юникс системы не стоят на месте. Они не только идеально подходят для серверных платформ, но также активно развиваются под мультимедиа и рабочие станции. Уже сейчас можно поиграть в популярные игрушки, изначально созданные под win32. Существуют большие офисные пакеты, вроде OpenOffice и StarOffice, а работа с Интернетом вообще проходит на ура! И, естественно, возникает желание познать все это самому, но тут-то и возникает подвох. При первых неудачах в изучении Unix системы пользователь возвращается обратно в "родные края" Windows'а, а продолжения познания того же Линукса можно и не дождаться. Но ведь так хочется быть гуру Юникса, а выход простой - берем 200/250 долларов, и вперед, на путь знаний :).

НАДО УЧИТЬСЯ

Будем записываться на платные курсы по Unix'у. Конечно, можно кричать, говорить, что научимся всему сами, но давай честно признаемся. Ведь гораздо проще, когда в тебя кто-то другой впихивает информацию, да причем все это разжевывая так, что и дурак поймет. Поэтому потратим какое-то количество денег, зато пройдем хорошие курсы по Unix. Курсы же мы будем проходить во всем известном институте МАИ. Почему именно МАИ? Во-первых, там недорогие курсы. И несмотря на довольно низкие цены, ты получишь отличные знания, а по окончанию выдадут диплом, которым можно похвастаться. Также размер группы очень мал, всего 6 человек, соответственно - не будет столпотворения, а на все вопросы получишь быстрые ответы. Т.е. индивидуальный подход к каждому. Правда, есть и один отрицательный момент. Курсы идут в течение пяти дней, с утра до вечера. Поэтому придется выделить всю неделю на обучение. Поверь, если ты только начинаешь изучать Linux или FreeBSD, то полученные знания очень помогут в будущем. Кстати, все преподаватели в общей массе своей бывшие студенты МАИ. Умные и молодые, так что я, как студент, быстро нашел с ними общий язык.

Список курсов

- ОС Linux для пользователя (250 у.е.)
- Администрирование ОС Linux (150 у.е.)
- ОС Linux в телекоммуникациях (250 у.е.)
- ОС Linux. Дистрибутив Mandrake/RE Spring 2001 (260 у.е.)
- Администрирование ОС FreeBSD (150 у.е.)
- ОС FreeBSD в телекоммуникациях (250 у.е.)
- Использование офисного пакета OpenOffice.org (200 у.е.)

Цены указаны для частных лиц, в случае юридического – цена увеличивается на 50 у.е.

В БОЙ, ЗА ЗНАНИЯМИ :)

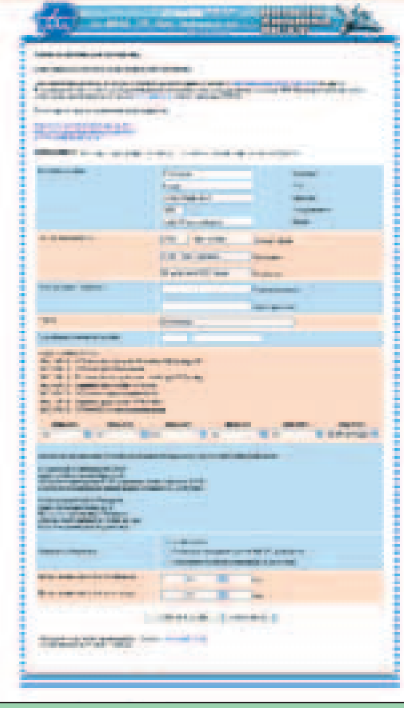
Если я уговорил тебя записаться на курсы, то первым делом заходи на сайт МАИ - http://www.mai.ru. Именно здесь оформляется заявка на прохождение курсов. Тебе предстоит выбрать, что ты хочешь пройти. Вот это уже решать самому. При нулевых знаниях записывайся на "ОС Linux для пользователя". При наличии знаний по работе в одной из этих двух систем (Linux и FreeBSD), смело записывайся на "Администрирование ОС Linux/FreeBSD". По этой программе тебя обучат глубинным настройкам Unix системы. Если же ты давно стал админом своей домашней машины под управлением Linux/FreeBSD и мечтаешь о высоком, например, администрировать небольшие сети, почтовые сервера и прочие серверные приложения, то выбирай программу "ОС Linux/FreeBSD в телекоммуникациях". Тебя обучат настройке маршрутизаторов, почтового сервера sendmail, dialup сервера, а также другим приятным в деле мелочам.

Все, выбор с типом курсов сделан. Дело за малым. Заполняй оставшиеся поля с ФИО, адресом проживания, паспортными данными. Данные отправлены, теперь придется подождать несколько дней, так как реагируют они не сразу :). По прошествию оных придет письмо с просьбой приехать к ним для оплаты и оформления договора. Оплата, естественно, производится в рублях. Место оплаты, как и место проведения занятий, находится на территории МАИ, т.е. это станция метро Сокол или Войковская (зеленая ветка сверху). У проходящих студентов спросишь, как добраться до ближайшей проходной (вход на территорию МАИ), а вообще в письме это будет подробно описано. После оплаты можешь готовиться к бою :)

Получив деньги, тебе выдадут бумажку для прохода. Кстати, с проходом на территорию МАИ вообще какие-то удивительные вещи происходят. Я почти все дни проходил, говоря, что иду на занятия по Линук-

су. Обычно меня пропускали, но попадались непонятные личности. Однажды один старичок гордо закрывал проход своей мужественной грудью и говорил, мол, кто ты такой и зачем идешь. В общем, не без странностей. Правда, в итоге оказалось, что вообще не на всех проходных пропускают.
Теперь о самих занятиях. Я проходил курс "ОС Linux в телекоммуникациях". Так что дальнейший рассказ пойдет об этом курсе, хотя он слабо отличается от "ОС FreeBSD в телекоммуникациях".

Первый день оказался самым трудным. Так как занятия начинаются в 9 утра, пришлось подниматься ни свет, ни заря, в 7 утра :). Для меня это сложно, особенно после ночных посиделок, так что лучше ложиться спать заранее, хоть выспишься. В итоге я немного опоздал, пришел сонным, но оказалось, что и сам преподаватель где-то задерживается. Из-за чего вместо рассказа об Internet провели лекцию по настройке X-Windows. Правда, после обеденного перерыва объявился преподаватель, и в оставшиеся часы группа слушала о таких сетях, как Internet и X.25.



Оформление заявки

Хочу обратить внимание, что занятия проводятся в небольшом помещении, где всего 6 компьютеров. Чувствуешь себя вполне уютно. Но вот очень не понравилась ситуация с едой. Естественно, питаешься за свой счет, поэтому тут два выхода. Либо брать множество продуктов с собой, что несколько неэтично, либо кушать в столовой МАИ. Я пошел в их столовую. Зверский голод после 5 часов занятий был утолен, но по возвращению домой случилось неприятное. Меня тошнило, а на следующий день из-за плохого самочувствия на занятиях не появился. Пришел только на 3-ий день. Преподаватели любезно поинтересовались причиной моего отсутствия, на что я им рассказал о прекрасной столовой. В ответ пошла монотонная речь, что быть такого не может.

На третий день мы занимались настройкой маршрутизаторов под управлением Linux. Этот день мне понравился больше всего, так как эта информация, скорее, вообще самая полезная из всего курса. На четвертый день занятий прошли изучения по настройке pppd сервера. Тоже очень интересно. Представь, у тебя дома выделенная линия и есть обычный модем для dialup соединений. Ты сможешь настроить у себя один пул с выходом в Интернет. Допустим, настроил. Едешь к другу. В настройках соединения устанавливаешь свой домашний телефон, прописываешь только тебе известные логин и пароль. Попадаешь в Интернет, наблюдаешь удивленные взгляды друга, дальнейшие просьбы объяснить все это. Наверное, это тщеславие :).

Расписание занятий

- Администрирование ОС Linux – с 16 по 20 сентября
- ОС Linux в телекоммуникациях – с 23 по 27 сентября
- ОС Linux для пользователя – с 30 сентября по 4 октября
- Администрирование ОС FreeBSD – с 14 по 18 октября
- ОС FreeBSD в телекоммуникациях – с 21 по 25 октября

В заключительный пятый день мы умудрились настроить почтовый сервер sendmail и Samba (NetBIOS сервер). После настройки sendmail я быстро вдохновился созданием своего почтового сервера @padonak.ru :). Хотя неясно, почему для разбора был выбран именно sendmail, ведь в нем постоянно находят ошибки, но дальнейший толчок к изучение почтовых серверов они дали. Далее за полтора часа мы умудрились настроить SAMBA и готовились расслабиться, как вдруг появился сам организатор курсов, доцент Бутко Анатолий Иванович. Пошло радостное повествование, итогом чего стало то, что наши знания уползли куда-то неимоверно далеко. В завершение каждому обучаемому были выданы сертификат об окончании курсов, дистрибутив RedHat 7.2 из 5 дисков, а также удостоились крепкого рукопожатия с доцентом :). Все радостны - курсы окончились.

Вот на этой оптимистичной ноте и заканчивается материал. Хочу добавить, что курсы мне действительно понравились. За все время обучения была приятная, ненагнетающая обстановка, все друг другу помогали. Так что при наличии денег и желании побыстрее освоить Unix записывайся. Лишних знаний не бывает.

Взлом

ИЩИ БАГИ В СЕБЕ!

Леший с Лукоморья (lukomore@real.xakep.ru)

Как искать ошибки в ПО, не прибегая к платным продуктам и услугам

ИЩИ БАГИ В СЕБЕ!

Если ты вдруг заболел гриппом или заподозрил у себя какую-то неизвестную болезнь, то первым делом (самолечение не в счет) обратишься к доктору, чтобы подтвердить или развеять свои опасения. Тем более, что медицина у нас бесплатная. А вот к кому обратиться, если "заболел" компьютер? Разумеется, к бесплатным сканерам, которые проверят твой компьютер на уязвимость.

Сразу отмечу, что бесплатный сыр бывает только в мышеловке и надо с определенной долей скептицизма относиться к результатам, получаемым на выходе этих сканеров. Однако применение продуктов от нескольких производителей позволит снизить до минимума риск того, что что-то будет пропущено. Также можно применять кряки к различным коммерческим решениям (например, Internet Scanner от ISS), но мы же законопослушные граждане и не будем нарушать лицензионную политику. Остается только применять бесплатные сканеры, например, X-Spider, ShadowSecurityScanner и т.д. Но... сканировать самого себя продуктом, который предназначен для дистанционной работы, - это "моветон". Тем более, что он покажет не совсем то, что нам нужно. Ведь тебя интересует взгляд на свою защищенность "со стороны", т.е. сканер должен размещаться на внешнем (по отношению к твоему компьютеру) узле. Если у нас есть дополнительный компьютер, на которой мы можем взгромоздить X-Spider, то нет проблем. А если такого компа нет? Не стоит унывать, в Internet полно различных платных и, что самое главное, бесплатных ресурсов, которые облегчают данную задачу. Поговорим именно о бесплатных решениях.

< Folder 1 >

ГЕЙТС ВСЕ ПРОВЕРИТ САМ

Первое, о чем я хочу рассказать, - это о решении компании Microsoft, которая в последнее время стала уделять безопасности своих продуктов немало внимания (http://www.microsoft.com/technet/security/default.asp).
Чего только стоят инициативы Secure Windows Initiative (цель - устранить дыры в продуктах до их доставки пользователю), Strategic Technology Protection Program (цель - помочь заказчикам в защите их Windows-систем) и Trustworthy Computing (цель - сделать софт и железо таким же надежным, как и электрооборудование).
Все это, конечно, хорошо, и такое начинание Microsoft не может не радовать, но... Microsoft и безопасность, на мой взгляд, вещи несовместимые. Несмотря на все заявления Билли о суперсистеме Prefix, осуществляющей автоматический поиск ошибок переполнения, об использовании RedTeam-тестов, передаче кода внешним компаниям для анализа и т.д., ошибки по-прежнему находятся, и число их не становится меньше. Как говорится, что-то надо делать. Видно, не будучи уверенным в том, что удастся сделать софт без неисправностей, соратники БГ выпустили несколько продуктов, предназначенных для поиска этих самых неисправностей. Итак, HFNetChk (Microsoft Network Security Hotfix Checker) - продукт, предназначенный для контроля непропатченных узлов, работающих под управлением Windows. Текущая версия 3.3 доступна для бесплатной загрузки по адресу: http://www.microsoft.com/downloads/release.asp?releaseid=31154. Сканирование осуществляется из командной строки, а проверке подлежит как локальный, так и удаленный компьютер. Разумеется, данная версия действует не для всех продуктов Microsoft, а только для:

- Windows NT 4.0
- Windows 2000
- Все системные сервисы, включая Internet Information Server 4.0 и 5.0
- SQL Server 7.0 и 2000 (включая MSDE)
- Internet Explorer 5.01 и выше.

Компания Microsoft также разработала еще одну утилиту - Microsoft Baseline Security Analyzer (http://www.microsoft.com/technet/security/tools/tools/mbsahome.asp), которая проверяет отсутствующие патчи и обновления для:

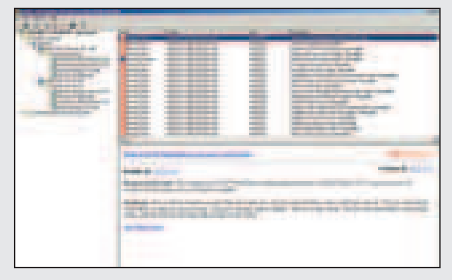
- Windows NT 4.0,
- Windows 2000,
- Windows XP,
- Internet Information Server (IIS) 4.0 и 5.0,
- SQL Server 7.0 и 2000,
- Internet Explorer (IE) 5.01 и выше,
- а также Office 2000 и 2002.

Еще можно встретить упоминания о таком продукте, как Microsoft Personal Security Advisor (MPSA). В настоящий момент он больше не существует, т.к. полностью заменен в апреле 2002 года продуктом MBSA, уже описанном выше.
Для проверки ОС, IIS и MS SQL используется HFNetChk. Другое отличие от HFNetChk - наличие графического интерфейса и функции генерации XML-отчетов. Текущая версия MBSA - 1.0.
Несмотря на объявление каких-то инициатив, было бы удивительным ожидать, что Microsoft выпустит в открытое плавание продукт для обнаружения дыр в своих же решениях. Кажется, что есть тут

какой-то подвох, и это действительно так. HFNetChk и MBSA разработаны совсем не Microsoft'ом, а совершенно другой компанией. Это Shavlik Technologies LLC (http://www.shavlic.com). Почувствуй разницу. Сама Shavlik предлагает расширенные версии этих продуктов (HFNetChkPro и EnterpriseInspector). В частности на странице http://www.shavlik.com/security/prod_hf_compare.asp приведена таблица сравнения HFNetChk с ее "профессиональной" версией, распространяемой, разумеется, за деньги. После ее изучения понимаешь, что никакими добрыми намерениями у Microsoft и не пахло. Только представь себе, что в мелкософтовской версии НЕТ:

- графического интерфейса;
- возможности работы по расписанию и выборочного сканирования узлов (по различным критериям, например, по продукту, по патчу, по типу сканируемого узла);
- загрузки патчей с сервера Microsoft;
- дистанционного размещения патчей, в т.ч. и между доменами (вот она, мечта любого админа);
- генерации отчетов в различных форматах (HTML, XML, CSV, PDF, Excel, Word, RTF и т.д.);
- хранения полной истории всех обновлений;
- создания своей логики работы HFNetChk;
- хранения результатов сканирования в MS Access или MS SQL Server.

Мало того, в версии от Microsoft и проверки-то не все проводятся. Иначе как понять фразу, что HFNetChkPro имеет возможность детальной проверки MS SQL и MS Exchange. Т.е. бесплатный HFNetChk обладает "знаниями" не обо всех дырках, в отличие от своего профессионального брата. Можно предположить, что Microsoft распространяет этот продукт только с одной целью - продвинуть платную версию компании Shavlik. Но применение и бесплатной версии не является пустой тратой времени - часто используемые дыры он обнаружит и укажет нам на них. А уж патчить их или нет - это остается на твоей совести.



HFNetChkPro собственной персоной

Многие пользователи, бродя по просторам Internet, используют ослика IE. Да что говорить, я сам его использую. Разумеется, понавесив на него кучу дополнительных примочек (например, MyIE), но ядро-то осталось от Microsoft. А Microsoft любит "облегчать" жизнь пользователям, интегрируя все свои продукты между собой. Так, например, из Internet Explorer можно просматривать документы Word'а, Acrobat Reader'а, Excel'а и т.д. Да мало ли еще чего можно делать, используя как широко, так и мало известные возможности IE. Тот же JavaScript или VBScript, ActiveX и DHTML и т.д. Все это может быть поюзано и для атаки на твой домашний комп, кражи файлов, удаления данных и т.п. Чтобы обезопасить себя от такого рода напастей, необходимо правильно настроить Internet Explorer (кстати, то же самое относится и к Outlook Express, и к Outlook), для чего я рекомендую следующие ресурсы:

- Проверка настроек ActiveX - http://users.rcn.com/rms2000/acctroj/axcheck.htm
- Проверка настроек интеграции браузера и Word'а - http://users.rcn.com/rms2000/acctroj/iframe.htm
- Проверка настроек интеграции браузера и Excel'а - http://users.rcn.com/rms2000/acctroj/excel.htm
- Проверка удаленного доступа к вашему Clipboard - http://users.rcn.com/rms2000/acctroj/clipmon.htm
- Проверка различных настроек компьютера и браузера - http://privacy.net/analyze/default.asp

После посещения указанных ссылок станет ясно, что является лишним на компьютере, а что стоит оставить. Первые из четырех указанных серверов подробно объясняют, к чему может привести наличие той или иной уязвимости на твоем компьютере, как ее может использовать хакер и, разумеется, как ее прикрыть.

АЛЬТЕРНАТИВНЫЕ СКАНЕРЫ

Интересные услуги предлагает сервер SecuritySpace (http://www.securityspace.com/sspace/index.html), который проводит как платное, так и бесплатное сканирование твоего узла на предмет выявления различных дыр (на момент написания статьи SS проводил проверку 992 уязвимостей). Нам предлагается несколько бесплатных вариантов аудита (No Risk Audit и Basic Audit), но, прежде чем воспользоваться ими, придется зарегистрироваться в качестве пользователя. Таким образом SecuritySpace пытается защититься от нелегального сканирования чужих адресов. Хочу сразу предупредить, что в бесплатной версии будут доступны не все проверки, но, как говорится, "на безрыбье и сам ... станешь". Помимо поиска уязвимостей, сервер "Безопасного пространства" также может просканировать наш узел на открытые порты с описанием каждого из них (и как их может использовать хакер), в т.ч. поддерживается работа через прокси-сервер. Кстати, далеко не все нижеперечисленные сервисы поддерживают эту возможность. Бесплатно на твоем компе будут проверены только 1300 портов, а вот чтобы узнать всю правду обо всех 65535 портах, придется башлять денег (креды принимаются ;). Также надо быть готовым к тому, что тест может занять до 5 часов - в зависимости от скорости твоего подключения к Интернету.

NEXT

Взлом

ИЩИ БАГИ В СЕБЕ!

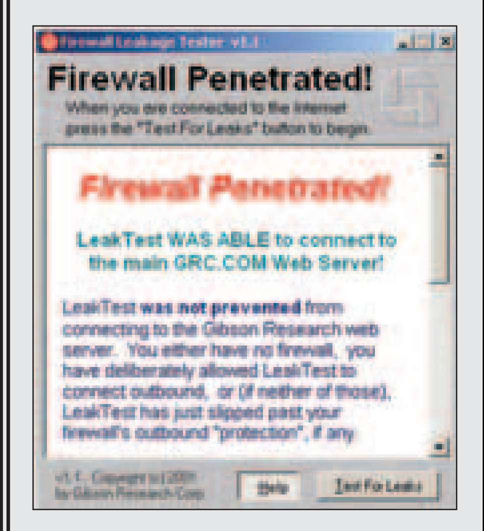
Леший с Лукоморья (lukomore@real.xakep.ru)

<Folder3>

ГИБСОН ТОЖЕ В ДЕЛЕ

Все читали "Нейромансера" Гибсона (о нем уже рассказывалось на страницах "Хакера")? Так вот, его однофамилец, создавший исследовательскую компанию, скромно названную Gibson Research Corporation (http://grc.com), предлагает нам два способа проверки своего компа:

- Сервис ShieldsUp (https://grc.com/x/ne.dll?bh0bkyd2), который в онлайне проверяет наличие открытого 139-го порта, расшаренных ресурсов NetBIOS и т.д. На моем компьютере все эти вещи удачно блокировались, что привело к появлению в отчете фразы: "This is very uncommon for a Windows networking-based PC" ("это очень необычно для Windows-машины") и "this computer appears to be VERY SECURE" ("этот компьютер, наверное, ОЧЕНЬ ЗАЩИЩЕННЫЙ").
- Утилиту LeakTest (http://grc.com/lt/leaktest.htm), которая пытается обойти защитные механизмы, реализованные во многих персональных межсетевых экранах.



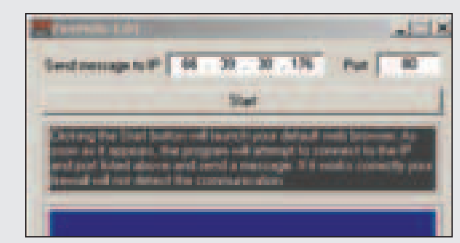
Утилита тестирование personal firewall LeakTest

НЕ СОВСЕМ НА ХАЛЯВУ

Кстати, можно воспользоваться сервисами компаний, которые предлагают аналогичные услуги на платной основе. Но для того, чтобы привлечь как можно больше покупателей, часть своих услуг (разумеется, не в полном варианте) они сделали бесплатными. К таким компаниям можно отнести:

- IT.SEC (http://www.it-sec.de/vulchke.html).
- Sygate (http://scan.sygate.com/). Эта компания известна своим одноименным персональным межсетевым экраном. По указанной ссылке мы получим возможность проведения TCP-, UDP-, ICMP-, Stealth-сканирования, а также поиска троянцев на компьютере.
- Broadband Reports (http://www.dslreports.com/scan).
- Symantec. По адресуhttp://security1.norton.com/ssc/home.asp?j=1&langid=us&venid=sym&plfid=22&pkj=RLLUBXUQIZQVMUYTACD можно в online-режиме проверить свой компьютер на наличие вирусов и широко известных уязвимостей. В отличие от других решений, с сайта Symantec на компьютер загружается небольшой код на ActiveX, который и проводит необходимые проверки изнутри.
- McAfee (http://www.mycio.com/asp_subscribe/trial_cc.asp), используя CyberCop Scanner.
- ProCheckUp (http://www.procheckup.com/tools/cgi/security.asp).
- Qualys (http://www.qualys.com/index.php?page=services).
- SecureDesign (http://www.sdesign.com/securitytest/index.html).

Кстати, если есть необходимость проверить свой фаервол "на вшивость", то, помимо LeakTest, можно использовать Tooleaky (http://tooleaky.zensoft.com/) и FireHole (http://keir.net/firehole.html). Сразу хочу добавить, что TooLeaky имеет небольшую ошибку. Она уведомляет о том, что фаервол обойден, даже если этого не произошло. Версия TooLeaky, которая не имеет этой ошибки, может быть найдена (с исходным текстом) по адресу: http://www.iss.net/security_center/tooleaky/.



Утилита тестирование personal firewall Firehole

Достоинство всех описанных служб в том, что они не требуют от тебя никаких дополнительных настроек. Достаточно просто перейти по указанной ссылке, после чего анализ и генерация отчетов производится автоматически. Характерно то, что создаваемые отчеты не доступны никому, кроме юзера, сканирующего самого себя. Тем самым гарантируется конфиденциальность информации о степени защищенности тестируемых компьютеров.

МАЛЕНЬКИЕ ХИТРОСТИ

Если ты сидишь за фаерволом, то тестироваться будет не твоя тачка, а фаервол. Т.к. брандмауер отсечет все подозрительные запросы, и они просто не дойдут до твоей машины.
Если ты тестишь порты и прочие уязвимости, то отключи в браузере прокси. Иначе, опять же, будет тестироваться прокси-сервер, а не твоя машина.
Вообще, любой онлайновый тест происходит вот так: ты заходишь на страничку, твой браузер передает серверу твой IP адрес, сервер начинает тестировать машину по этому IP. Т.ч. для теста именно своей машины сделай все, чтобы предоставить серверу именно свой IP, а не прокси-сервера, фаервола или локального сервера.
Для локальщиков: если у вас нет внешнего IP, то чаще всего вы обломаетесь с тестами.



<Взлом>25/08\02

TIPS&TRICKS

В некоторых матерях (в ASUSовских точно) есть полезная штучка - переключив джампер, который обычно находится недалеко от Power Connector'a и называется KBPWR, комп можно запускать клавишей пробел (при условии, что компьютер подключен к питанию и форм-фактор ATX). Это удобно, если доступ к кнопке Power затруднен.

Shag Shagoff <shag0s@rambler.ru>

Взлом

ГОРЯЧАЯ ДВАДЦАТКА

Леший с Лукоморья (lukomore@real.xakep.ru)

Двадцать самых распространенных ошибок всех времен и народов

Горячая двадцатка

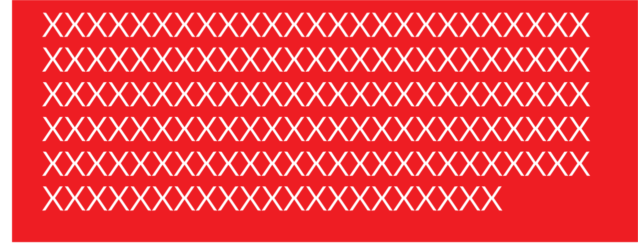
< Folder 1 >

Когда ты заходишь на очередной сайт "нашей" тематики (PacketStorm, SecurityFocus, Insecure и т.д.), то наблюдаешь огромное множество информации об ошибках в различном софте. Число таких ошибок исчисляется тысячами, и разобраться, что же использовать для взлома, становится непосильной задачей. Можно посмотреть и с другой стороны. От чего надо защищаться в первую очередь, какие ошибки чаще всего используются? Ответ на этот вопрос был бы нетривиален, но… Существуют еще на свете добрые ребята, сделавшие за нас всю работу. Я говорю о горячей двадцатке ошибок всех времен и народов.

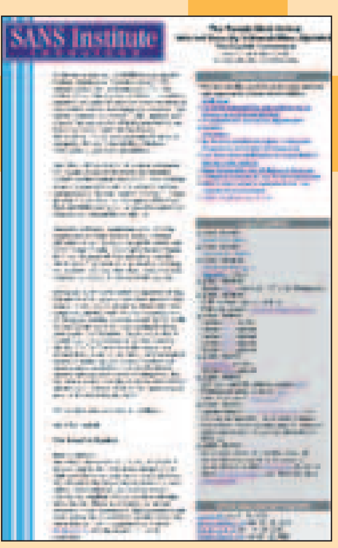
ЛЕКАРСТВО ОТ МОРЩИН

Очень часто от админов можно услышать об их состоянии в вечной запарке, отчего не успевают отследить все ошибки и пропатчить их. Мало того, они не знают, какие ошибки самые опасные, чтобы прикрыть их в первую очередь. Для помощи администраторам в 2000 году две американских конторы - институт SANS (http://www.sans.org) и Центр защиты национальной инфраструктуры (http://www.nipc.org) опубликовали горячую десятку уязвимостей "The Top 10 Most Critical Internet Security Threats List", которая достаточно регулярно обновлялась. В основу данного списка легли статистические данные различных государственных и военных организаций, коммерческих компаний и исследовательских центров и т.д. 25 июня 2001 года была опубликована последняя (1.33) версия данного списка (http://www.sans.org/topten.htm), после чего он благополучно скончался. Перечислю уязвимости, вошедшие в последний релиз горячей десятки:
* Слабость BIND (nxt, qinv и in.named)
* Уязвимые CGI-скрипты и приложения на Web-сервере (например, ColdFusion)
* Дыры в RPC (rpc.ttdbserverd, rpc.cmsd и rpc.statd)
* RDS в IIS
* Переполнение буфера в sendmail и MIME
* Уязвимость в sadmind и mountd
* Расшаренные ресурсы в Windows (порты 135-139 для NT и 445 для W2k), Unix (порт 2049) и MacOS (порты 80, 427 и 548)
* Отсутствие или слабые пароли пользователей, в т.ч. и админов
* Переполнение буфера в IMAP и POP
* Заданные по умолчанию common string SNMP - public и private.

1 октября 2001 года родился новый проект, в основу которого легла безвременно ушедшая десятка, - Top20 (The Twenty Most Critical Internet Security Vulnerabilities). В отличие от Top10, соавтором SANS при создании горячей двадцатки стало ФБР США (http://www.fbi.gov). Рост числа уязвимостей (особенно после событий 11 сентября и эпидемии Nimda и Red Code) привел к тому, что число рассматриваемых в списке уязвимостей удвоилось, и они были разделены на 3 класса:



* уязвимости "вообще" (General Vulnerabilities),
* уязвимости Гейтса, точнее его детищ (Windows Vulnerabilities),
* юникс уязвимости (Unix Vulnerabilities).



Sans Top20

Горячая двадцатка также регулярно обновляется - последняя доступная версия (http://www.sans.org/top20.htm) - 2.504 от 2 мая этого года. Рассмотрим ее более подробно. Начну с ошибок, присущих всем системам, независимо от их производителя.

ЛУЧШАЯ ДЫРКА ВСЕХ ВРЕМЕН И НАРОДОВ

Первое место по праву занимает установка ОС и софта по умолчанию. Наверное, не стоит лишний раз говорить, что настройки, заданные производителем, надо менять и как можно скорее. Это относится и к Windows, и к Unix, и даже к сетевому оборудованию. Если ты думаешь, что в Oracle, Sun, Cisco сидят люди, которые за тебя решат твои же проблемы, то ошибаешься. Точнее - они их решат, но не бесплатно и не сразу. Как говорится, "доверяй, но проверяй". Поэтому лучше лишний раз проверить свою систему, чем потом искать виновных и посыпать голову пеплом после потери ценных данных. Тем более, что многие организации свободно распространяют различные чеклисты (бенчмарки), позволяющие быстро защитить свою систему. Одной из таких контор является Центр Internet-безопасности, который предлагает 6 чеклистов - для Windows NT, Windows 2000, Solaris, Linux, HP UX и Cisco IOS. Например, один из распространенных взломов роутеров Cisco - вход на него по дефолтовому, админскому паролю.
Кстати, с этой ошибкой связана и другая уязвимость, поставленная SANS на второе место, - слабые или отсутствующие пароли. К чему это может привести - говорить не стоит. Тем более, что существуют средства, автоматизирующие подбор паролей (о них я уже писал в 3-м номере Хакера).

ВСЕ ЗАКРЫТЬ, ЧТОБ НЕ ПОРУТИЛИ

На третье место специалисты SANS и FBI поставили отсутствие бэкапа, то бишь резервного копирования, что может привести к тому, что после атаки системы восстанавливать ее содержимое будет не с чего. 4-е место принадлежит слишком большому количеству открытых на компьютере портов, что облегчает злоумышленнику проникновение на него. Следуй правилу - "все, что не разрешено, - запрещено". Зачем открытый 80-й

порт, если ты не предоставляешь Web-сервис своим друзьям? Чем меньше лазеек оставишь на своем компьютере, тем выше его защищенность и меньше вероятность, что взломают.

Пятерку "поставили" отсутствию фильтрации исходящих и входящих адресов, которая могла бы быть включена на персональном или корпоративном межсетевом экране (firewall). Не стоит облегчать жизнь злоумышленнику, допуская в сеть или на компьютер пакеты с такими Internet-адресами, как 192.168.x.x, 10.x.x.x, 172.16.x.x и т.п. Эти пакеты никогда не могут встретиться в Internet, поэтому их необходимо смело блокировать. Существуют и другие примеры адресов, которые не стоит пускать к своему компьютеру, - более подробно они описаны в книге А. Лукацкого "Обнаружение атак" (в книжном обзоре Хакера о ней уже писали). Отсутствие или неполная регистрация событий также входит в список самых опасных ошибок. И это правильно. Если ничего не фиксировать, то и обнаруживать следы хакерской деятельности очень затруднительно. Замыкают семерку лидеров уязвимые CGI-скрипты, которые позволяют дефейсить Web-сайты, красть с них номера кредиток и выполнять другие неприятные действия.

ЭТО НЕ ДЫРКА, ЭТО ЦЕЛАЯ НОРА!

Ошибки в Windows как обнаруживались, так и обнаруживаются, и ничего тут не поделать. Надо только знать, какие являются самыми распространенными. Эпидемии Nimda и Red Code лишний раз показали миру "доброе" лицо Билла Гейтса. Первые три места занимают уязвимости IIS:

* всем известная ошибка в Unicode (т.н. Web Server Folder Traversal)
* переполнение буфера в ISAPI Extensions
* уже упомянутый выше IIS RDS.

Четвертое место досталось расшаренным ресурсам, доступным по NetBIOS, а пятое - утечке информации через "нулевой сеанс" (null session). Они применимы как к ранним версиям ОС Windows, так и к их более старшим сестрам (например, Windows 2000). Шестую позицию занимает механизм хэширования паролей в Windows (LM hash), уязвимость которого позволяет достаточно быстро узнать пароли пользователей. В чем заключается уязвимость этого механизма? Во-первых, алгоритм шифрования паролей в LAN Manager достаточно слабый. Во-вторых, независимо от длины выбранного пароля, Windows его обрежет до 14 символов, да еще и переведет его в верхний регистр и... разобьет на два пароля поменьше (по 7 символов). Что в результате? Надо сломать всего 2 семисимвольных пароля, да еще в верхнем регистре (т.е. число возможных комбинаций уменьшилось почти вдвое). Седьмое место в данной категории пустует. Но не потому, что у мелкософта больше нет ошибок, а потому, что ребята из SANS решили, что раз их список зовется Top20, то тремя семерками придется пожертвовать и сделать две семерки и одну шестерку.

ЮНИКС ТОЖЕ БАЖИТ... ПО-ЧЕРНОМУ

Юниксовая семерка лидеров начинается с ошибок в RPC, причем особой популярностью пользуется переполнение буфера в трех демонах:

* rpc.ttdbserverd (ToolTalk)
* rpc.cmsd (Calendar Manager)
* rpc.statd.

Можно заметить, что в Top10 дыры RPC находились только на третьем месте, но за два года ситуация в корне изменилась. Уязвимый BIND переместился с первого места на третье, а второе место захватила sendmail. Доверенные отношения, широко используемые в Unix, позволили R-командам (rlogin, rsh, rcp) занять четвертое место. Проникновение на один из доверенных узлов автоматически дает вам возможность получения контроля и над другими машинами.
Переполнение буфера в демоне in.lpd, отвечающем за работу принтера, может привести к выполнению вредоносного кода, чем нередко пользуются злоумышленники. Эта ошибка встречается на различных Solaris'ах и многих Linux'ах, что позволило данной уязвимости занять почетное пятое место.
Шестое место, как и в горячей десятке, занимают уязвимости sadmind и mountd, а замыкает семерку - заданные по умолчанию SNMP string. И хотя SNMP используется не только в Unix, эксперты, составлявшие список Top20, зафиксировали большое число проникновений в Unix-системы именно по причине недооценки опасности SNMP.

А ТЕПЕРЬ ТЕЛО В ДЕЛО

На этом двадцатка самых распространенных уязвимостей завершается. Я надеюсь, что ты, прочитав этот материал, сделал выводы и твоя машина не станет взломанной очередным "хакером". Почаще следи за багтраками в Интернете, латай дыры, и успехов тебе на поприще компьютерной безопасности.

HACK-FAQ

Horrific (hack-faq@real.xakep.ru)

Задавая вопросы, конкретизируй их. Давай больше данных о системе, описывай абсолютно все, что ты знаешь о ней. Это мне поможет ответить на твои вопросы и указать твои ошибки. И не стоит задавать вопросов вроде "Как сломать www-сервер?" или вообще просить у меня "халявного" Internet'а. Я все равно не дам, я жадный :)

<???> Когда я сижу в халявном Инете, может ли тот, на чьем счету я сижу, войти в сеть, когда я тоже онлайн?

Н: Возможно - да, а может - и нет. Все зависит от наличия у прова определителя номера или нормально настроенного софта. Если пров мелкий, то и админы чаще всего бывают не совсем образованные, тогда сервер просто не отслеживает, что по одному аккаунту лезет несколько челов. Хотя пару лет назад я купил себе ночной анлим, и мы втроем с приятелями выходили по этому логину в Сеть одновременно безо всяких ограничений. И при этом пров был не маленький, а 2-й или 3-й по величине в городе. Так что тут однозначного ответа дать нельзя, это надо проверять в каждом конкретном случае.

<???> Расскажите, пожалуйста, про вирус Win32.VCell, а то я его подхватил, а как избавиться, не знаю :(.

Н: А зачем от него избавляться? Лично я считаю, что таких вирусов, как этот, должно быть как можно больше :). Он всего лишь ищет startup файлы и безобидно дописывается в конец. Ну а 30-го числа каждого месяца ты увидишь какое-нибудь сообщение, после чего запустится IE (или другой браузер) и загрузится порнографический сайт. Так что теперь у тебя каждое 30-е число будет праздником души и тела :).

<???> Вы не подскажете, чем ядро Unix'a отличается от ядра Windows?

Н: А чем отличается мышь от слона? И то, и другое - животные, но в остальном они разные. Точно так же и тут - ядра Unix и Windows - это ядра, но больше у них ничего общего нет. Да, в них есть отдельные схожие блоки, например, блок управления памятью, которые выполняют похожие функции, но выполняют они их по-разному. Так что тут легче сказать, чем они схожи, чем описать отличия.

<???> Какими прогами можно разогнать проц?

Н: Самая лучшая программа - BIOS или «Перемычки на мамке 1.0». Хотя встречаются проги и под Windows, но они заточены под определенные версии мамок, и далеко не каждая мать настраивается из-под форточек (даже если существует софт конкретно под нее). Так что если на диске к мамке ничего не было и на сайте производителя про софт для настройки параметров BIOS ничего не сказано, то лучше забудь про эту идею. Если ты запортишь какой-нибудь безымянной тулзой свой комп, то я не хочу нести за это ответственность.

<???> Недавно я с помощью BlackICE обнаружил, что мои порты кто-то сканирует. BlackICE выдал мне айпишник этого чела, и я с помощью хуиза решил проверить, кто это. Сервер оказался провайдеровским! Вопрос: нафига им это надо? И имеют ли они право этим заниматься? И вообще, в сканировании портов есть что-либо противозаконное?

Н: Ну, на счет противозаконности я не могу ничего сказать. Наше законодательство - это такая черная дыра, в которой даже адвокаты и судьи с трудом разбираются. Но лично мое мнение - в этом нет ничего противозаконного (по крайней мере, по нашим законам). А вот по законам этики я считаю это неправильным. Раз тебя сканируют, значит, им что-то нужно. Раз это пров, значит, он может собирать о тебе какую-то инфу (например, пользуешься ли ты проксиком), а это не этично.
Ну а теперь самое главное - ты уверен, что найденный тобой IP принадлежит серверу? То, что он принадлежит прову, еще не значит, что это сервант. Ты попробуй проверить свой IP и увидишь, что он тоже принадлежит прову. Так что это может быть простой юзер, который решил стырить твои пароли.

<???> Как извлечь адрес мыла, на который будут идти пароли из троянов?

Н: Тут вариантов миллион. Если твой троянец собран с помощью конструктора или собственными руками, то адрес чаще всего находится в открытом виде в каком-нибудь файле настроек или в самом запускном файле. Можешь попробовать открыть троян с помощью любого просмотрщика и запустить поиск по символу @. Очень часто такой способ дает положительный результат, потому что 80% «писунов» троянов не обладают большими знаниями в кодинге или просто не заботятся о какой-либо защите. Единственная проблема, с которой ты можешь столкнуться, - это если файл сжат какой-нибудь прогой для сжатия PE файлов. В этом случае нужно узнать прогу архиватор и найти к ней деархиватор. Если это сложно сделать, то могу посоветовать воспользоваться отладчиком. Хорошие отладчики умеют разархивировать все распространенные архивы.

<???> Я просканировал сервак и заметил, что на 139-м порту стоит NetBIOS Session Service. До этого я точно был уверен, что на серванте установлена *nix система, а теперь уже и не знаю, что думать. Если это *nix, то почему же открыт 139-й порт?

Н: Если открыт 139-й порт, то это еще не значит, что на серванте окна. В *nix этот порт тоже может быть открыт. Ты, наверно, уже не раз слышал слово SAMBA - это NetBIOS сервер для Linux. С помощью этого сервера Linux машина может работать так же, как и оконная. Это значит, что любой юзер сможет видеть расшаренные ресурсы Linux в сетевом окружении Windows и монтировать их как сетевые диски. Вот именно этот сервер и открывает 139-й порт.
Тут другое странно - если сервер инетовский, то зачем там запущена самба? Любой админ сервера, подключенного к инету, должен руководствоваться правилом: «Каждый лишний открытый порт - дополнительная дверь для хакера». А 139-й порт - явно лишний, тем более, что его защищенность оставляет желать лучшего. Так что или админ ламер, или это засада.

<???> Если я закажу товар в Инет-магазине на адрес своего друга, то ребята из «Управления Р» придут к нему или ко мне?

Н: Нет, они придут ко мне :). Ну, конечно же, первым под подозрение попадет твой друг, и его первого повяжут. Но не надо думать, что это отличный способ западлостроения, потому что если ребята из «Управления Р» захотят, то оправдают твою жертву в пять сек. Во-первых, это покажет проверка компа. Во-вторых, это покажет проверка логов магазина (там всегда сохраняется IP адрес, с которого заказали товар) и логов прова (какой IP и у кого из его юзверей был в этот момент). Так что парня оправдают, а вот тебя ждут большие неприятности, если по IP они смогут выйти на тебя.

<???> Это правда, что в Windows XP есть встроенный файервол? Если да, то каковы его возможности и как его включить?

Н: Действительно, есть такая штука от Билла Гейтса, и она должна быть включена по умолчанию. Только вот возможности данной проги очень ограничены. Максимум, что может сделать эта стена, - отбить примитивную атаку на твой комп. Встроенный в XP FireWall предназначен только для отклонения несанкционированных подключений к твоему компу извне. Избавиться от баннеров с его помощью невозможно, да и любой троян, поселившийся у тебя, беспрепятственно сможет отправлять пароли куда угодно, потому что соединения, идущие от имени твоего компа, не контролируются. Так что не советую сильно рассчитывать на дядюшку Билли.

<???> Объясни, пожалуйста, почему, когда я выключаю (или просто перезагружаю) комп из Win2k, он мне (секунд через 6-7) пишет «Beginning dump of physical memory» и не реагирует ни на что, кроме резета, хотя из WinME и WinXP выходит без проблем.

Н: Скорей всего, проблема в каком-то драйвере или сервисной службе, которая не может нормально завершить работу. Просто во время выхода она приводит к сбою в системе, и происходит сохранение текущего состояния памяти, чтобы потом ты мог определить, что глюкнуло (но это достаточно сложное занятие).
В качестве выхода могу посоветовать отключить Dump памяти. Для этого щелкаешь правой кнопкой по «Мой компьютер» и входишь в свойства. Здесь на закладке «Дополнительно» щелкаешь по кнопке «Параметры» в разделе «Загрузка и восстановление». Вот здесь и отключаешь Dump памяти. После этого комп не будет так критично относиться к глюку, хотя проблема все равно остается.

Эти вопросы меня уже достали

Я уже давно создал на своем сайте www.cydsoft.com/vr-online раздел «Большой FAQ», где я выкладываю все часто задаваемые вопросы и ответы. Прежде чем задавать мне вопрос, посмотри, может на сайте уже есть ответ.

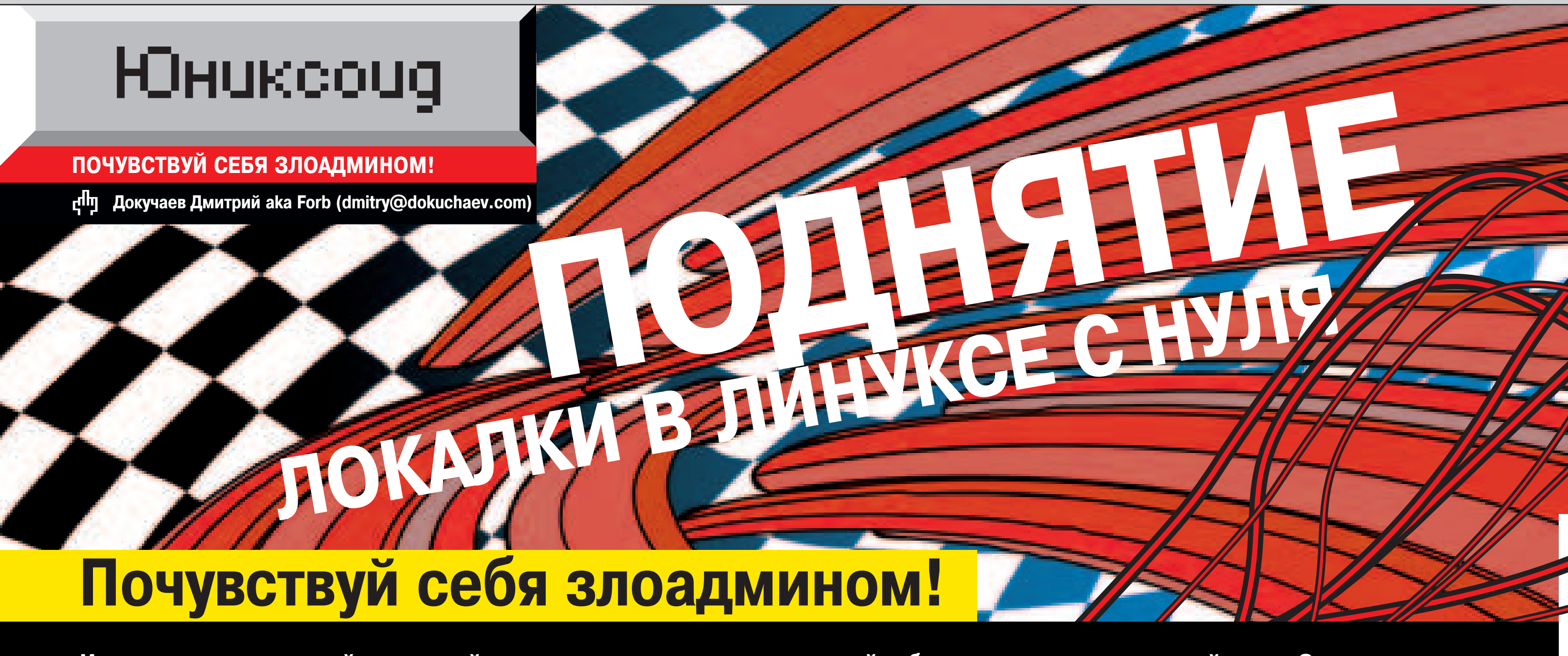
<???> С помощью чего я могу подключиться к удаленной тачке на какой-либо открытый порт?

Н: Один из самых регулярно задаваемых вопросов. В апрельском номере Х я достаточно подробно расписал, что такое порты. После этого я надеялся, что подобные вопросы закончатся, но не тут-то было.
Каждый открытый порт - это какая-то серверная программа. Просто сетевые проги для передачи данных в сеть открывают порт и используют его для приема/передачи. Вот отсюда и вытекает ответ. Раз порт открыла серверная прога, то и присоединиться к нему можно с помощью клиентской проги для этого сервера. Например, если открыт 21-й порт, то, значит, там сидит FTP Server. А для соединения с ним используется FTP Client.
Ко многим портам можно еще присоединяться с помощью Telnet клиента. В этом случае ты сможешь после соединения отправлять серверу его команды в простом консольном режиме. Опять же, если это FTP сервер, то и отсылать ему придется FTP команды, которые описаны в любом RFC.



ПОЧУВСТВУЙ СЕБЯ ЗЛОАДМИНОМ!

Докучаев Дмитрий aka Forb (dmitry@dokuchaev.com)



Почувствуй себя злоадмином!

Итак, в один прекрасный солнечный день ты скопил денег на недорогой хаб и пару сотен метров витой пары. Затем, протянув локальную сетку с друзьями во дворе, в первую очередь ты должен усвоить одно важное правило: сеть без сервера - не сеть, даже если это простая "дворовая" сеть из 3-4 компьютеров. Если ты миллионер и желаешь поддержать дядюшку Билли, пополнив его карман "вечнозелеными" за удобный сервак на NT, то можешь смело пропускать эту статью. Я же рассмотрю процесс создания сервера сети в Linux с нуля, где, как известно, на высоком уровне развит TCP/IP-протокол и сервисы, что дает полную свободу выбора программного обеспечения и методов настройки. Не забуду затронуть и настройку всех необходимых сервисов для локалки, чтобы всем было сухо и комфортно =).

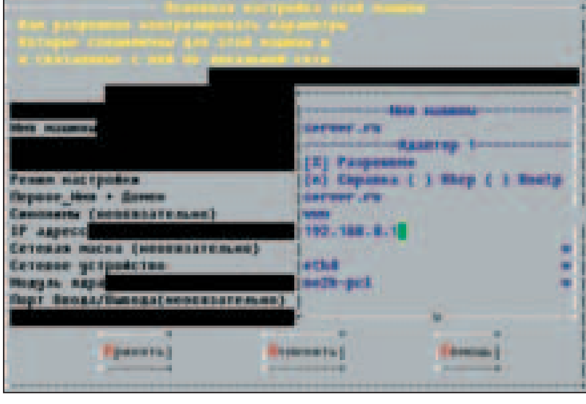
В конце концов ты выбрал Linux - в качестве сервера твоей домашней сети (в данной статье я опишу один сервак на несколько клиентских машин). Бытует мнение, что пингвиненок Тукс более подходит для рабочих станций, а для сервера лучше использовать FreeBSD. Это мнение я оспаривать не собираюсь, но для меня проще поднять локалку именно в Linux, вдобавок учитывая тот факт, что большинство стандартных сетевых программ ориентировано все-таки для твоего любимого Пингвина. Начнем, как водится, с нуля. Для начала было бы неплохо установить свежий дистрибутив Linux на отдельную машину в твоей сети, которая впоследствии и будет сервером.

Рисуем картину сети

Первое, что нам необходимо сделать, это то, чтобы сервер видел все работающие машины в твоей сети (пока на уровне IP-адресов). Дадим твоей локальной сети, в качестве примера, диапазон адресов в подсети 192.168.0.0/24 (то есть от 192.168.0.1 до 192.168.0.24). Сервер, безусловно, должен иметь адрес 192.168.0.1 (так как это все же главный компьютер). Для настройки локального IP-адреса сервера убедимся, что сетевая карта находится в PCI-слоте и работает (проверить наличие карты можно командой "dmesg | more" - при загрузке системы все устройства пишутся в консоль).

Далее, запускаем приложение /bin/netconf. Нас интересует первый раздел в этой программе - "основная информация о машине". Туда прописываем следующие параметры для сервера сети:

Имя сервера - server.ru (в дальнейшем server.ru - имя твоего сервера)
IP-адрес - 192.168.0.1
Маска сети - 255.255.255.0
Сетевое устройство - eth0
Модуль ядра: ne2k-pci (как правило, работает со многими картами, если не будет работать - попробуй модуль 8139too либо смотри дискету, прилагающуюся к сетевухе)



Производим основные настройки сервера

Внимание, важное обстоятельство! Клиентские машины должны иметь такую же маску подсети и адреса по возрастанию в подсети 192.168.0.0/24 (192.168.0.2, 192.168.0.3 и т.д.).

При выходе из netconf все изменения вступят в силу без перезагрузки (это тебе не Виндовс :). Проверить правильность настройки можно обычным пингом: ping 192.168.0.1, далее пингуй рабочие машины в твоей сети. Если на пинг по какой-то причине не приходит ответ, то ты что-то настроил не так (в первую очередь читай /var/log/messages).

Настройка DNS

Помни, что сервер без сервисов - не сервер, поэтому на компе обязательно должны стоять несколько важных сервисов. В первую очередь - named DNS-server.
Про настройку named'а можно писать целую книгу, поэтому я изложу лишь то, чего будет достаточно для настройки твоей локальной сети.

В первую очередь настроим DNS-клиент сервера (машина должна знать, к какому DNS-серверу ей обращаться). Для этого пишем в /etc/resolv.conf:

```
domain server.ru
search 192.168.0.1
nameserver 192.168.0.1
```

Этим мы настраиваем DNS-клиент.

Далее идем править сам named, а точнее его конфиги, которых несколько. Смотри:

I. /etc/named.boot

Дописываем в этот файл 2 строки, которые служат для настройки прямого и обратного резолва IP-адресов:

```
primary     server.ru     server.ru.zone
primary     0.168.192.in-addr.arpa  192.168.0.rev
```

II. /etc/named.conf

Сюда вписываем название зон и пути к соответствующим файлам:

```
zone "server.ru"{
	type master;
	file "server.ru.zone";
};
zone "0.168.192.in-addr.arpa"{
	type master;
	file "192.168.0.rev";
};
```

Такой конструкции будет достаточно - останется лишь прописать хосты на соответствующие IP-адреса. Если изучить /etc/named.boot, то можно увидеть, что там прописывается путь к файлам, содержащим в себе информацию о зонах. Это по умолчанию директория /var/named, поэтому, не медля, переходим в нее. Там создаем 2 файла (touch "192.168.0.rev" "server.ru.zone").

LINUX - ОДНА ИЗ ЛУЧШИХ ОСЕЙ ДЛЯ СЕРВЕРА СЕТИ, ПОТОМУ ЧТО ПИНГВИН ОБЛАДАЕТ:

1) Многопользовательским режимом со средствами защиты данных от несанкционированного доступа.
2) Пластичной настройкой сервисов и взаимодействия нескольких сетей (включая InterNet).
3) Кэшированием диска с целью уменьшения среднего времени доступа к файлам.

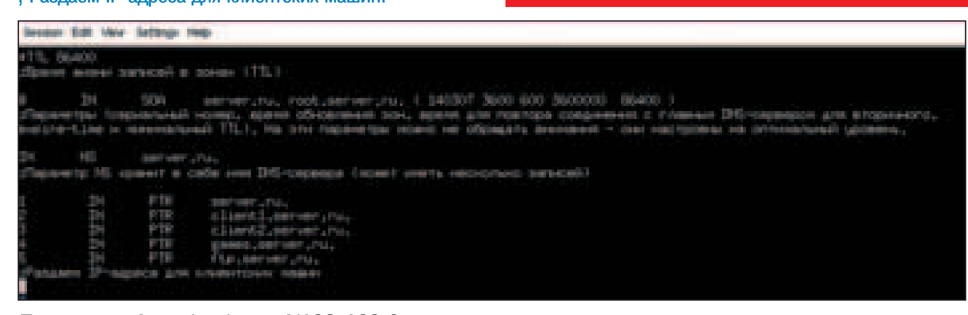
III. /var/named/192.168.0.rev

Вот как выглядит файл, преобразующий IP-адрес в host:

```
$TTL 86400
; Время жизни записей в зонах (TTL).
@	IN	SOA	server.ru. root.server.ru. ( 140307
3600 600 3600000  86400 )
; Параметры (сериальный номер, время обновления
зон, время для повтора соединения с главным DNS-
сервером для вторичного, expire-time и минимальный
TTL). На эти параметры можно не обращать внимания
- они настроены на оптимальный уровень.

IN	NS	server.ru.
; Параметр NS хранит в себе имя DNS-сервера
(может иметь несколько записей).

1	IN	PTR	server.ru.
2	IN	PTR	client1.server.ru.
3	IN	PTR	client2.server.ru.
4	IN	PTR	games.server.ru.
5	IN	PTR	users.server.ru.
; Раздаем IP-адреса для клиентских машин.
```



Пример конфига /var/named/192.168.0.rev

TTL для зоны следует указать обязательно. Далее идет указание primary DNS-сервера и перечисление IP-адресов и хостов на каждую клиентскую машину.

IV. /var/named/server.ru.zone
В этом файле закладывается обратное преобразование: host -> ip

```
$TTL 86400
@	IN	SOA	server.ru. root.serv-
er.ru.  ( 140307 3600 600
3600000 86400 )

@	IN	NS	server.ru.
@	IN	A	192.168.0.1
; Это позволит обращаться с любого
компьютера в сети к самому себе,
используя зарезервированное имя serv-
er.ru.

$ORIGIN server.ru.
ns	IN	CNAME	server.ru.
www	IN	CNAME	server.ru.
irc	IN	CNAME	server.ru.
; CNAME - алиас для одного и того же компьютера - в
данном случае server.ru

client1	IN	A	192.168.0.2
client2	IN	A	192.168.0.3
client3	IN	A	192.168.0.4
users	IN	A	192.168.0.5
; Записываем реверс IP-адресов в соответствующие
имена.
```

ПОЧЕМУ MASQUERADE БЕЗОПАСНЕЕ SQUID?

С помощью IP Masquerade можно подключить к Интернету компьютеры, которые не имеют зарегистрированных IP-адресов, через шлюз с Linux. При этом будет работать большинство протоколов, но снаружи компьютеры во внутренней сети не будут видны. С помощью же Squid будут проходить только http- и ftp-запросы.

После изменений (либо первых составлений) в этих файлах, следует перезапустить named командой "killall -1 named"
Запускать демон нужно при старте машины (для этого достаточно написать "ln -s /etc/rc.d/init.d/named /etc/rc.d/rcX.d/S45named", где X - текущий runlevel машины).

Учитывай важное обстоятельство: всем клиентским машинам в свойствах локальной сети следует прописать первичный DNS-сервер 192.168.0.1.

Мутим Интернет

После того как все успешно зарезолвилось и заработало (если нет, то подними глаза выше и перечитай все заново), пора расслабиться и настроить выход в глобал. Разумеется, на сервере должен быть выход в Интернет (через модем либо через выделенный канал - последнее, конечно, предпочтительней =). Тебе, как админу своей, хоть и не большой сетки, просто необходимо дать всем пользователям, а не только себе, возможность выхода в Инет и от души там повеселиться =). На этот случай есть 2 варианта. Либо поставить proxy-server, либо воспользоваться встроенным файрволлом Ipchains. Остановимся на втором варианте.

Для удобства работы напишем небольшой скрипт маскарадинга, работающий через Ipchains. Его следует запускать при каждом старте сервера.

```
#!/bin/bash
test -x /sbin/ipchains || exit 1
case $1 in
   start|restart|force-reload)
    echo -n "Включаем IP Masquerading"
    echo 1 > /proc/sys/net/ipv4/ip_for-
ward
## Включаем forward для проброса
пакетов изнутри наружу.
    /usr/sbin/routed -q
## Включаем роутинг для внутренней
подсети.
   /sbin/ipchains -P forward DENY
## Запрещаем forward для всех адресов.
   /sbin/ipchains -A forward -s
192.168.0.0/255.255.255.0 -j MASQ
## Разрешаем masquerade для локальной сети
192.168.0.0/24 с соответствующей ## маской
255.255.255.0
   echo "done."
   ;;
stop)
   ;;
esac
```

После активизации данного скрипта будет включен маскарадинг на всю подсеть, и все юзеры, собственно, смогут юзать Инет через главный сервер.

NEXT

Юниксоид

ПОЧУВСТВУЙ СЕБЯ ЗЛОАДМИНОМ!

Докучаев Дмитрий aka Forb (dmitry@dokuchaev.com)

На вершине безопасности

Интернет тесно соприкасается с безопасностью. Чтобы никто не смог порутить твой сервак через Инет, нужно запретить все соединения извне. Тут Ipchains снова приходит к нам на помощь. Записываем новое правило, к примеру, запрещающее все коннекты на SSH извне:

ТРИ ЗАВЕТНЫХ КРИТЕРИЯ СЕТИ:

1) Локалка без сервера - не локалка.
2) Сервер без сервисов - не сервер.
3) Каждая локалка - это свой мини-интернет.

```
# /sbin/ipchains -I input !192.168.0.0/24
192.168.0.0/24 22 -p tcp -j REJECT
```

После этого никто снаружи не сможет зайти на сервер, хотя сервак будет, как обычно, находиться в сети.

Можно запретить таким же образом все icmp-запросы (пинги), обращенные к серверу:

```
# /sbin/ipchains -I input !192.168.0.0/24
192.168.0.0/24 -p 1 -j REJECT
```

Согласно rfc, icmp первый в списке протоколов.

Вообще, мы о безопасности в Линуксе неоднократно писали, поэтому отсылаю тебя за деталями к статье Cordex'а из 4-ого номера X этого года.
Просто соблюдай все правила безопасности, и тогда твой сервер будет "недоступен" как снаружи, так и изнутри. Да-да, не забывай, что юзеров локалки хлебом не корми - дай что-нибудь поломать ;).

Это я - почтальон Печкин

В любой нормальной локалке (а я верю, что ты хочешь, чтобы у тебя была именно такая) должна быть грамотно настроена почта.
В Linux по дефолту входит postfix (улучшенный вариант sendmail).
По умолчанию все работает, но опять же на 90% :).
Тебе останется лишь изменить параметры в конфигурационном файле, чтобы mail-server не кодировал письма с русским текстом.
Для этого зайди в файл /etc/mail/sendmail.cf, найди секцию SMTP Mailer specification и поменяй поля F=mDFMuX на F=mDFMuX8 и F=mDFMuXa на F=mDFMuXa8.



Короче, мой типс гнилой и старый, правда, когда посмотрел на моих друзей за работой в Юникс, понял, что гнилой, да не воняет пока, чтоб все чувствовали :). В Баше (Бурн Шеле, оболочке *никсов) можно делать некоторые вещи, которые помогут писать и читать быстрее и удобнее:
1) Чтобы не набирать вручную длинный файл типа win4lin-mat_tvoju_za_nogu-4.0-2.4.8-26.i586.rpm... достаточно набрать несколько первых букв и нажать табуляцию.
2) Текст в окне консоли можно прокручивать нажатием Шифт+ПагДаун.
3) Клавиши Вверх и Вниз помогают не вводить недавние команды.
4) Тильда в имени директорий означает домашнюю директорию.
Можете ваще не помещать мои гнилые советы, только не делайте рубрику "Самые тупые советы месяца"! :)

Nixen Nixen@email.ru

После этого в директории /etc/mail надо создать файл relay_domains, в который вписывай все домены, на которых будет настраиваться почта. В данном примере - server.ru.

Но это только половина почтовых сервисов. Чтобы юзеры могли снимать свою почту, тебе нужно установить POP3-демон. Рекомендую тебе поставить демон popa3d. Несмотря на странное название ;), эта малютка выполняет всю черную работу, не жрет ресурсов и практически не ломается (лично я не видел для popa3d ни одного эксплойта).
Чтобы демон поставился, следует немного поправить файл Makefile, а именно разремить флаг -lcrypt для линкера.
Затем записывай его в inetd (или xinetd) как сервис pop-3.
Если ты юзаешь inetd, то запиши в /etc/inetd.conf что-то вроде:

```
pop-3  stream tcp   nowait root   /usr/sbin/tcpd
/usr/sbin/popa3d
```

И рестартни inetd ("/etc/rc.d/init.d/inet restart").
После этого пробуй телнет на 110-ый порт сервака (в случае успеха - popa3d выдаст "+OK").

```
Session  Edit  View  Settings  Help
[root@home /root]# telnet 192.168.0.1 110
Trying 192.168.0.1...
Connected to 192.168.0.1.
Escape character is '^]'.
+OK
user test
+OK
pass test
+OK
list
+OK
.
stat
+OK 0 0
quit
+OK
Connection closed by foreign host.
[root@home /root]#
```

Производим основные настройки сервера

Если что-то не работает, прочти логи - "tail /var/log/messages", - там будет написана подробная причина ошибки.
Один пользователь может иметь несколько почтовых ящиков. Алиасы пишутся в файле "/etc/aliases".
Формат алиасов примерно следующий:

```
alex: alex@mail.ru
serj: client3
```

Как ты видишь, алиасы могут быть как прямыми, так и редиректами, что дает большой плюс почтовой системе. Ну и, конечно, после всего вышеизложенного попробуй послать какому-либо пользователю почтовое сообщение, дабы убедиться в правильности настроек.

World Wide Web на локальном уровне a la WWW & FTP

Полмира знает, что самый популярный WWW-сервер - это, конечно же, Apache. Он хорошо поддается настройке, снабжен огромным количеством модулей и удобен в юзабельности :). Но описывать подробности его настройки я не буду, т.к. это было сделано до меня в X, да и в Инете инфы дофига.
Теперь насчет FTP. Разумеется, для того чтобы пользователи могли заливать файлы на сервер, нужно поставить FTP-Daemon. Рекомендую взять свежую версию ProFtpd (дыр меньше, а возможностей больше). С его настройкой особо заморачиваться не стоит (все настроено на более-менее безопасном уровне). Кстати, любого желающего ты сможешь прописать в Access Denied =) в файле /etc/ftpusers.

На IRC-овку становись!

Итак, ты настроил named, ftpd, www, pop3, smtp... На душе стало веселее, пользователи сети довольны, и ты ощущаешь себя настоящим системным администратором! Но чего-то не хватает... Правильно - общения. Поэтому бери ноги в руки и бегом ставить IRC-сервер. Знай, что после того как пользователи сети привыкнут к IRC, они тебе за такую услугу будут ставить халявное пиво и носить на руках =).
Что касается софта, лично я рекомендую поставить PTlink IRCD. Взять свежую и пропатченную русскими кодерами версию можно отсюда: http://aldem.net/irc. PTlink имеет дружелюбный интерфейс и стандартную настройку. Там же ты найдешь и описалово к серверу, и правила линковки в крупную IRC-сеть. Если ты протянешь выделенку к твоему серваку - то можешь слинковаться с сетью irc.ircnet.ru (проходящий трафик небольшой, а пользователей очень много - проблем с коммуникабельностью не возникнет =).

И это все?

И, наконец, последнее правило - нет одинаковых серверов! Все зависит от фантазии злоадмина, то бишь твоей =). Никто тебе не запрещает экспериментировать с новым софтом на твоем серваке. Если у тебя руки растут откуда надо - ты справишься и создашь комфорт любому пользователю из твоей сети, что тебе с лихвой и окупится. Поэтому, не откладывая, задумайся - что ты хочешь от своей сети и в каком направлении собираешься ее развивать.


Silvershield
Silvershield
Phone
Line
Protection
fault
«Silver Shield»
специально разработан
для защиты дорогостоящей
электронной аппаратуры
Безопасность:
• Розетки оборудованы защитными шторками
• Тумблер питания с коммутацией двух проводников
Самодиагностика:
• Индикация выхода из строя системы защиты от сетевых помех
• Автоопределение фазы и нуля в розетке
• Индикация подключения к розетке с дефектной шиной заземления
Многоуровневая защита от сетевых помех:
• Фильтрация высокочастотных и импульсных помех
• Фильтрация помех радиочастотного диапазона
• Защита телефонной линии от импульсных помех
Эргономичный дизайн:
• Специальная розетка для подключения громоздких адаптеров питания и вилок старого российского образца
• Три цвета на выбор: серебристый металлик, черный, светло-серый
Гарантия 3 года
Спрашивайте в магазинах Москвы:
«Формоза», ул. Авиамоторная, д.59,
Компьютерный супермаркет «НИКС», Звездный б-р, д. 19,
«Пирс» ООО, Кронштадский б-р, д. 37, к. «Б», оф. 133,
«Ф-Центр», ул. Сухонская, д. 7а,
Компьютерный центр «Буденовский», пр-т Буденного, д. 53,
«Ситилинк», ул. Народного Ополчения, д. 34,
Ну что, Пилоты? Удивлены?

UNIX-FAQ

Если у тебя возникли какие-либо вопросы Unix-тематики, то, не раздумывая, мыль мне: unixfaq@real.xakep.ru. Главные требования к вопросам: не повторяйся, будь как можно более конкретным и кратким в своем вопросе, задавай только те вопросы, на которые сам не можешь найти ответ. Я постараюсь осветить их, насколько это будет в моих силах, в ближайших выпусках UnixFAQ'a.

Andrushock (andrushock@fromru.com)

Q. Я получаю такое сообщение об ошибке при запуске программы в иксах: Xlib: connection to ":0.0" refused by server Xlib: Client is not authorized to connect to Server Gtk-WARNING **: cannot open display: :0 Хотя, когда сижу под root'ом, подобной проблемы нет. Что делать?

A. У тебя просто отсутствуют права доступа для подключения к X-серверу. Для управления списком имен пользователей и хостов, которым требуется разрешить/запретить возможность коннектиться, служит утилита xhost. Командой xhost +localhost ты разрешишь всем локальным пользователям получить заветный доступ, а для конкретного пользователя, например, хакер'а, используй: xhost +local:xakep.

Q. Сижу в пингвине, все хорошо, все нравится, вот только ужасный звук сильно раздражает. Как его отключить?

A. Не нравится звук? Нет проблем! В иксах прекрати свои мучения строчкой: xset b off ; для тишины в консоли набивай: setterm -blength 0 -bfreq 0 . Чтобы каждый раз их не вводить, первую прописывай в конфигурационный файл .xinitrc (при запуске иксов скриптом startx), а вторую в один из стартовых скриптов твоей системы, например, /etc/rc.local.

Q. Как мне быстро найти нужную программу в дереве портов и можно ли передать какие-нибудь параметры для ее сборки? Если можно, то как?

A. Итак, ищем архинужную в хозяйстве прогу, возьмем, к примеру, xmms: cd /usr/ports make search key=xmms . Все. Результаты поиска будут у тебя на экране. Переходи в нужный каталог: cd audio/xmms, и набирай: env FLAVOR=no_gnome make install clean (если ты используешь Bourne shell). Этим ты себя обезопасил от выкачки половины Gnome :). Все возможные аргументы для данного порта ты сможешь посмотреть в правиле сборки (Makefile), найдя в нем ключевое слово FLAVORS.



Q. Хочу научиться писать программы с использованием GTK! С чего начать?

A. Лавры xchat не дают покоя? :) Что ж, для начала тебе нужен сам gtk+ и gtk+-devel, в последнем, кстати, есть неплохой туториал и пара десятков примерчиков. В теории подсобить также поможет сайт производителя: www.gtk.org. Если ты собираешься заниматься еще и 3D-графикой, то без специальной библиотеки Mesa (www.mesa3d.org) тебе никак не обойтись, которая представляет собой практически точную копию OpenGL от Silicon Graphics, Inc. Дерзай!

Q. Как работать с буфером обмена в иксах? Copy&Paste не пашет :(.

A. Для помещения одного слова в буфер достаточно подвести к нему указатель крысы и нажать быстро два раза левую кнопку, для целой строки - три раза, для выделения некоторого фрагмента текста перемести указатель мыши к его началу и, удерживая левую кнопку, дотяни до его конца. Для вставки текста из буфера дави средний кнопарь (или колесо мыши); если он отсутствует, то одновременно нажми на левую и правую кнопки. Видишь, как все просто :). Но помни: помещенный фрагмент текста в буфер можно использовать до тех пор, пока ты его не перезапишешь новым фрагментом.

Q. Как заставить работать ролик крысы в иксах?

A. Ищи в своем конфиге иксов раздел с параметрами мыши Section "InputDevice" и дописывай: Option
"Buttons" "5" Option
"Emulate3Buttons" "no" Option
"ZAxisMapping" "4 5"

Q. Проблемы с транспарент прокси! Пакетики попадают на Squid, а он возвращает броузерам, что, типа, не может открыть страницу "http://".

A. Ты на верном пути. Просто в squid.conf добавь эти четыре строчки, и все будет в шоколаде: httpd_accel_host virtual httpd_accel_port 80 httpd_accel_with_proxy on httpd_accel_uses_host_header on

Q. При отсутствии в каталоге файла index.html (или что указано в директиве DirectoryIndex) веб-сервер Apache выводит оглавление этого каталога в табличном виде. С колонками Name, Last modified, Size все понятно. А вот как прописать Description для файлов, а то лениво пагу делать?

A. Для этого должен быть подгружен модуль autoindex.c . Проверь сначала, есть ли у тебя такие строчки в httpd.conf: LoadModule autoindex_module modules/mod_autoindex.so AddModule mod_autoindex.c А теперь лезь в описание твоего каталога (допустим, /var/www/html/xakep) и прописывай: <Directory "/var/www/html/xakep"> Options Indexes IndexOptions FancyIndexing # включаем режим описания файлов AddDescription "Диалапный сниффер" super-proga.tar.gz # задаем описание для файла super-proga.tar.gz AllowOverride None Order allow,deny Allow from all </Directory> Остается лишь заново перезапустить Апач и наслаждаться :).


Модемы серии
OMNI 56K
Модем • Факс • Автоответчик • АОН
EDITORS' CHOICE
V.92/V.44 - максимальная скорость доступа в Интернет
Надежность связи на любых линиях
Легкость установки – простота в обращении
Возможность обновления микропрограммы
ИНТЕРНЕТ С РЕКОРДНОЙ СКОРОСТЬЮ
OMNI 56K PRO
OMNI 56K DUO
OMNI 56K NEO
OMNI 56K PCI
Товар сертифицирован
ZyXEL
www.omni.ru

Horrific aka Фленов Михаил (smirnandr@mail.ru)
www.cydsoft.com/vr-online

Delphi Смена видеорежима

По многочисленным просьбам сегодня мы научимся программно менять видеорежимы Windows. Помимо этого, я покажу, как вытаскивать из системы список возможных видеорежимов, чтобы ты случайно не выбрал невозможное для моника сочетание параметров.

Horrific aka Фленов Михаил smirnandr@mail.ru www.cydsoft.com/vr-online

Дизайним форму

Для примера нам понадобятся на форме один компонент ListBox и две кнопки. По нажатию первой кнопки мы будем выдирать из системы все возможные варианты видеорежимов и записывать их в ListBox. По нажатию второй кнопки мы будем делать активным режим, выделенный в списке ListBox. Можешь расположить все компоненты, как угодно, а можешь сделать, как я (см. рисунок 1).

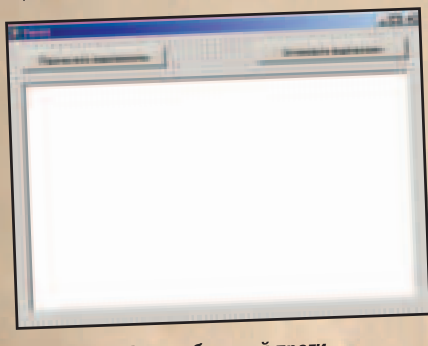


Рисунок 1. Форма будущей проги

Итак, на первой кнопке напиши что-нибудь типа «Перечислить видеорежимы», а на второй - «Установить видеорежим». Теперь прога выглядит более солидно, и можно приступать к шкодингу.

Прежде чем написать какой-то код, надо объявить массив из переменных типа TdevMode, в котором мы будем сохранять параметры найденных видеорежимов. Для этого находим раздел private и пишем в нем:

```
private
  { Private declarations }
  modes:array[0..255] of TDevMode;
public
  { Public declarations }
```

Этим я объявил массив из 255 элементов типа TDevMode.

Перечисление режимов

Для начала создаем обработчик события OnClick для кнопки и пишем в нем следующий текст:

```
procedure TForm1.Button1Click(Sender: TObject);
var
 i: Integer;
begin
 ListBox1.Items.Clear;
 i := 0;
while EnumDisplaySettings(nil, i, Modes[i]) do
  begin
   ListBox1.Items.Add(IntToStr(Modes[i].dmBitsPerPel)+' '+
        IntToStr(Modes[i].dmPelsWidth)+' '+
        IntToStr(Modes[i].dmPelsHeight)+'  '+
        IntToStr(Modes[i].dmDisplayFrequency));
   Inc(i);
  end;
 end;
```

В первой строке кода я очищаю содержимое списка ListBox с помощью вызова ListBox1.Items.Clear.

В следующей строке я обнуляю переменную i, которая будет использоваться в качестве простого счетчика и указывать, какой по счету видеорежим нам нужен. Дальше я вызываю функцию EnumDisplaySettings, которая перечисляет доступные системе видеорежимы. У этой функции три параметра:

1. Устройство, для которого надо перечислять режимы. Здесь нужно что-то указывать только тогда, если у тебя несколько мониторов. Если ты простой смертный с одним моником, то можно смело указывать nil.
2. Здесь указываем индекс режима, который нам нужен. Я указываю переменную i, которая перед каждым вызовом будет увеличиваться на 1, а значит, мы будет каждый раз получать следующий по счету режим.
3. Переменная типа TDevMode, в которую нужно записать параметры режима. Сюда я каждый раз подставляю очередной элемент из массива.

Вызов функции происходит между операторами while и do:

```
while EnumDisplaySettings(nil, i, Modes[i]) do
```

Это значит, что пока результат вызова функции EnumDisplaySettings не станет ошибкой, будет выполняться последующий между begin и end цикл. В этом цикле я добавляю строку в список ListBox, в которой записаны параметры найденного режима, и увеличиваю счетчик i на единицу.

Когда я добавляю новый элемент в список ListBox, то в качестве строки я передаю следующую информацию:

Modes[i].dmBitsPerPel - глубина (количество бит на пиксель) цвета найденного режима.
Modes[i].dmPelsWidth - ширина экрана.
Modes[i].dmPelsHeight - высота экрана.
Modes[i].dmDisplayFrequency - частота развертки.

Проверим!!!

Можешь теперь запустить этот промежуточный вариант нашей проги и нажать на кнопку «Перечислить видеорежимы». Список ListBox должен заполниться строками, содержащими информацию о найденных видеорежимах (рисунок 2).

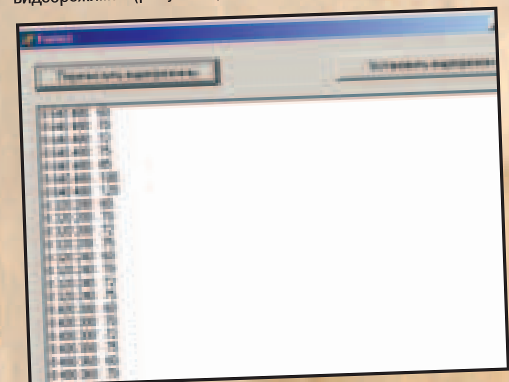


Рисунок 2. Результат перечисления видеорежимов

Все строки разбиты как бы на четыре колонки:

1. Глубина (количество бит на пиксель) цвета найденного режима.
2. Ширина экрана.
3. Высота экрана.
4. Частота развертки.

ОТ РАБОТЫ ПО НАЙМУ - К ФИНАНСОВОЙ НЕЗАВИСИМОСТИ

журнал **уже в продаже**

СВОЙ БИЗНЕС



Нужен ли такой журнал?

На вопрос "Нужен ли такой журнал?"

92% опрошенных ответили - ДА

8% ответили- НЕТ

О чем этот журнал?

Первый в России толстый ежемесячный журнал, полностью посвященный малому предпринимательству. В нем на конкретных примерах описываются проблемы, с которыми сталкиваются индивидуальные предприниматели и небольшие компании. А квалифицированные эксперты предлагают возможные пути их решения.

В чем отличие от других журналов

«**Свой бизнес**» печатает информацию интересную для малого предпринимательства, и смотрит на все события глазами предпринимателей. В нем нет экономических скандалов и политической трескотни. О бизнесе рассказывается доходчивым языком – интересно и понятно даже тем, кто не силен в экономической теории.

В чем польза этого журнала?

Морально и практически помочь россиянам, решившим открыть свое дело. Журнал дает возможность найти кратчайший путь к успеху и избежать множества ошибок при открытии своего бизнеса.

СУПЕРАКЦИЯ

В первом номере журнала объявляется конкурс бизнес-планов «Открой свой бизнес!» Его победители получат до $3000 долларов, чтобы начать свое дело. Главные условия конкурса: предложить перспективный проект и регулярно вести предпринимательский дневник, выдержки из которого будут публиковаться в журнале.



- Изменения в законодательстве о малом бизнесе
- Обзоры перспективных рынков для малого предпринимательства
- Практические советы о том, как начать свое дело
- Рекомендации экспертов: как решать типичные задачи, встающие перед предпринимателями
- Ответы консультантов на вопросы предпринимателей
- Налогообложение и кредитование малого бизнеса
- Обзоры оборудования, необходимого для ведения бизнеса
- Безопасность бизнеса
- Формирование команды и управление персоналом
- Психология бизнеса
- Опыт и ноу-хау зарубежного малого бизнеса
- Истории современников, которые начали свой бизнес с нуля и сумели добиться успеха
- Истории знаменитых промышленных и торговых династий дореволюционной России
- Обзор полезной деловой литературы и сайтов Интернет



СМЕНА ВИДЕОРЕЖИМА

Horrific aka Фленов Михаил (smirnandr@mail.ru)
www.cydsoft.com/vr-online

Смена видеорежима

По нажатию второй кнопки «Смена режима» мы должны установить выделенный в списке режим. Для этого по нажатию второй кнопки пишем следующий код:

```
procedure TForm1.Button2Click(Sender: TObject);
begin
 Modes[ListBox1.ItemIndex].dmFields := DM_BITSPERPEL or
    DM_PELSWIDTH or DM_PELSHEIGHT or
    DM_DISPLAYFLAGS or DM_DISPLAYFREQUENCY;
ChangeDisplaySettings(Modes[ListBox1.ItemIndex], CDS_UPDATEREGISTRY);
end;
```

ListBox1.ItemIndex - указывает на выделенный элемент в списке. Это значит, что для того, чтобы найти нужную структуру для выделенного элемента, в массиве Modes надо записать Modes[ListBox1.ItemIndex]. Все достаточно просто, потому что элементы в списке ListBox1 находятся в том же порядке, что и соответствующие структуры TDevMode в массиве Modes.

Прежде чем менять видеорежим, надо в структуре Modes заполнить свойство dmFields, в котором указывается, что именно менять. Здесь ты можешь указать сочетание следующих флагов:

1. DM_BITSPERPEL - будет меняться количество бит на пиксель.
2. DM_PELSWIDTH - будет меняться ширина экрана.
3. DM_PELSHEIGHT - будет меняться высота экрана.
4. DM_DISPLAYFREQUENCY - будет меняться частота развертки.
5. DM_DISPLAYFLAGS - изменить флаги дисплея.

Если ты хочешь поменять только количество бит на пиксель (глубину цвета), то в свойство dmFields достаточно указать только DM_BITSPERPEL. Я буду менять все, поэтому перечислил все флаги через оператор «or», который объединяет все в одно целое.

После заполнения этого свойства можно вызывать процедуру ChangeDisplaySettings. У нее два параметра:

1. Структура типа TdevMode.
2. Флаги.

В качестве флага можно указать одно из следующих значений:

1. Ноль - если просто поставить ноль, то разрешение экрана изменится динамически.
2. CDS_UPDATEREGISTRY - в этом случае разрешение также изменится динамически, но с обновлением параметров в реестре.
3. CDS_TEST - если указать этот флаг, то произойдет только тест возможности переключения видеорежима. Реального переключения не будет.

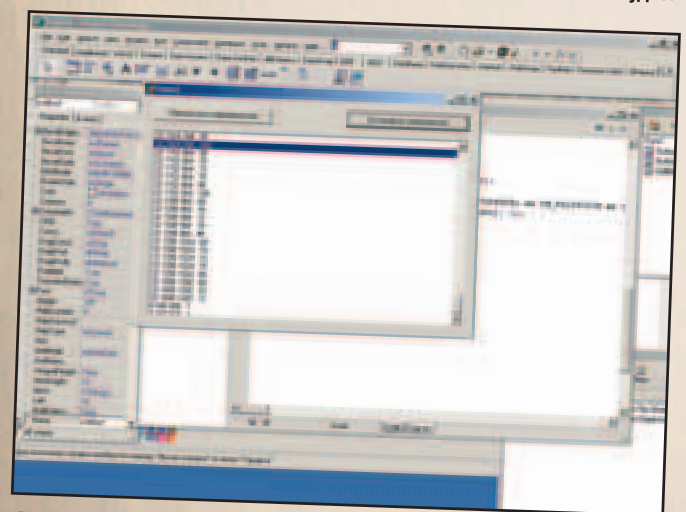


Рисунок 3. Смена режима на меньший при флаге, равном 0

Побочный эффект

Очень интересный эффект происходит при смене видеорежима, если указать в качестве флага 0. В этом случае режим меняется, но окна не реагируют на эту смену и остаются в том же положении. Посмотри на рисунок 3, на котором я сменил режим на меньший и при этом исчезла панель Windows с кнопкой «Пуск». Она просто не отреагировала на смену режима. На рисунке 4 показан экран, на котором я, наоборот, сменил режим на больший, и тут также панель не отреагировала и осталась на много выше нижней части экрана.

Disconnect

Некоторые считают, что если часто менять разрешение экрана, то можно его испортить или спалить. Да, такое возможно, но только на старых мониторах. Современные моньки защищены от такой примитивной атаки, так что такой вирус не прохляет.

Но если включить свою соображалку на большие обороты, то можно придумать какой-нибудь более существенный прикол. Например, многие моники выводят чер-

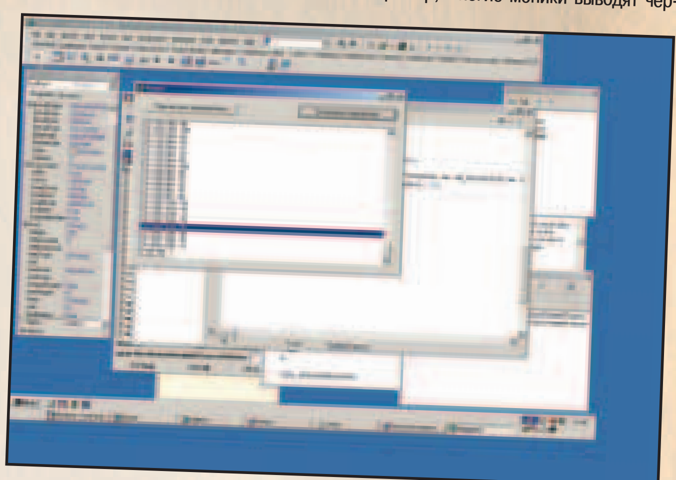


Рисунок 4. Смена режима на больший при флаге, равном 0

ный экран с надписью об ошибке, если попытаться установить неправильные параметры видеорежима. Это значит, что можно написать прогу, которая будет менять режим на недопустимый, и поместить ее в автозагрузку. Теперь при каждой загрузке прога будет менять режим, и моник автоматом будет уходить в даун, а значит - пользователь не сможет работать :).

На этом смену видеорежима считаю оконченным. Как всегда, исходники примера будут доступны на моем сайте www.cydsoft.com/vr-online после выхода этого номера в свет, а те, у кого нет Инета, могут найти их на нашем диске.

P.S. У меня к тебе просьба, на сто баксов :). Не пиши мне большие письма. После появления рубрики кодинг меня каждый день валят вопросами. Я не в состоянии всем рассказывать то, о чем пишут книги. Я могу что-то подсказать, где-то помочь, но не больше. А просьбы типа помоги написать прогу вообще нереальны. Я отвечаю только на те вопросы, где ответ займет несколько строчек. Целые лекции по мылу я разводить не могу. Я бы с удовольствием помог всем, но это НЕВОЗМОЖНО. Вас слишком много, а я один :(((. Поэтому лучше разбей свой вопрос на несколько маленьких и спрашивай постепенно, а не все сразу.

TIPS&TRICKS

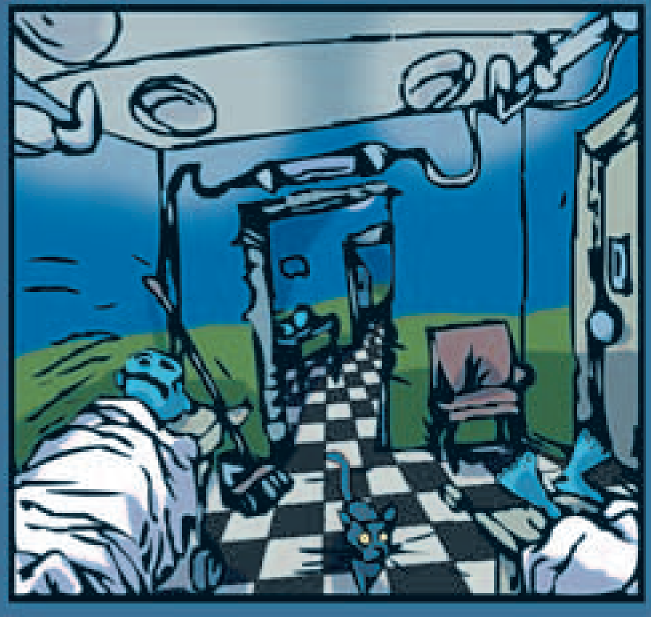
Если в Windows в окно Калькулятора вставить из буфера обмена строку чисел, разделенных знаками простейших арифметических действий (+, -, *, /), оканчивающуюся знаком равенства, то калькулятор автоматически вычислит последовательно все действия, и на его "индикаторе" появится результат, который, при необходимости, можно легко перенести в любое работающее приложение Windows посредством того же буфера обмена. Результат вычислений, выполняемый по такой методике, зависит от того режима, в котором находится Калькулятор. В обычном режиме строка символов воспринимается как простая последовательность нажатий соответствующих клавиш, не отдавая приоритета операциям умножения и деления. В инженерном виде вычисления производятся по всем правилам, можно даже использовать скобки и некоторые специальные последовательности символов-кодов, выполняющих служебные функции, например:

:q Начало нового вычисления.
:c Очистка памяти.
:e Ввод десятичных чисел в экспоненциальной нотации.
:m Запоминание числа в памяти.
:p Добавление текущего числа к хранящемуся в памяти.
:r Вызов числа, хранящегося в памяти.

Garik http://www.webhowto.ru/reg

Ведущий рубрики Tips&Tricks Иван Скляров (Sklyarov@real.xakep.ru)


МОРГ










100,5

Horrific aka Фленов Михаил (smirnandr@mail.ru)
www.cydsoft.com/vr-online

Первая анимация

Как я и обещал, сегодня мы создадим первую спрайтовую анимацию. Спрайты долгое время были основой в игровой графике, да и демомейкеры их не обходили стороной. Поэтому их понимание необходимо и обязательно для любого кодера компьютерной графики.

Horrific aka Фленов Михаил smirnandr@mail.ru www.cydsoft.com/vr-online

Теория

Спрайтовая анимация - это просто копия мультипликации. Как создается мультик? Сначала рисуется персонаж. Чтобы заставить его двигать рукой, нужно просто нарисовать много картинок, где рука персонажа будет медленно изменять свое положение. Теперь если быстро пролистать все картинки, то получается плавное движение рукой.

Компьютерная анимация похожа на мультипликацию. Посмотри на рисунок 1. На нем нарисован самолет, постепенно меняющий угол наклона. Если быстро пролистать каждый из кадров да еще и заставить кадры двигаться по оси X, то получится ощущение, что самолет летит.

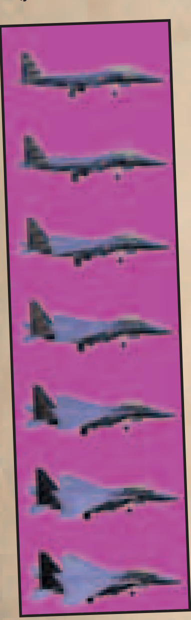


Рисунок 1. Анимация самолета

Именно таким способом создавались первые компьютерные игры. Ты думаешь, что в первом Doom монстры действительно были трехмерными? Нет, тогда мощности компьютеров на это не хватало. Просто дизайнеры подготовили большое количество картинок монстров в разных ракурсах, а программеры заставили нас поверить в трехмерность этих картинок. Ловкость рук и никакого обмана.

Преданимационный период

Итак, чтобы заставить нашу анимацию двигаться, нам понадобятся следующие дополнительные переменные:

X и Y - в этих переменных будет храниться текущее положение самолета.

State - состояние самолета. Я подготовил картинку из 7 положений самолета, и эта переменная будет указывать, какое именно положение сейчас должно отображаться.

LastXState - это для хранения времени, когда последний раз менялось состояние самолета. Так как самолет должен двигаться по оси X (т.е. лететь слева направо), то здесь будет храниться X позиция. Состояние будет меняться, когда он пролетит по оси X на очередные 10 пикселей.

incparam - эту переменную я буду использовать для хранения значения приращения состояния самолета. Ну и сказанул. Короче, вначале здесь будет храниться 1. Когда надо изменить состояние, то я просто прибавляю это приращение к переменной State (State:=State+incparam). Это значит, что переменная State будет увеличиваться. Когда самолет получает состояние 7 (отображается 7 картинок), мне надо будет сделать так, чтобы переменная State стала уменьшаться, чтобы состояние самолета отражалось в обратном порядке. Для этого я меняю incparam на -1, и теперь State:=State+incparam будет уменьшать значение State.

К взлету готов

Загружай пример из предыдущего номера X, сейчас мы его подкорректируем. Для начала надо приготовиться к взлету и всем новым переменным присвоить начальные значения. Для этого где-нибудь в начале старта приложения (лучше даже до кода, создающего окно) написать:

```
incparam:=1;
x:=0;
LastXState:=0;
y:=random(400);
```

Переменной Y я присваиваю значение функции random, которая возвращает случайное число в диапазоне от нуля до числа, переданного в качестве единственного параметра. Конечно же, высоту полета можно было бы задать и постоянным числом, но я решил сделать его случайным. Пускай самолет летает где хочет, лишь бы не разбился :).

Цикл сообщений

Теперь надо подправить наш цикл обработки сообщений. Раньше он был неэффективен, потому что выглядел так:

```
while (GetMessage(msg, 0, 0, 0)) do
 begin
 end;
```

Здесь мы получали очередное сообщение от ОС с помощью GetMessage и обрабатывали его. А что если сейчас нет для нас сообщений? Программа просто застывала на вызове функции GetMessage и могла ждать бесконечно.

Для компьютерной графики более эффективно будет использовать функцию PeekMessage, которая проверяет, есть ли для нас сообщение. Если есть, то она возвращает true, а если нет, то результатом будет false. С использованием этой функции логика обработки сообщений изменяется так:

1. Запускаем бесконечный цикл (while true do).
2. На каждом этапе цикла проверяем с помощью PeekMessage, есть ли для нас сообщения.
3. Если нет, то можем заниматься своими делами, если да, то обрабатываем их.
4. Возвращаемся на пункт 2 и снова проверяем наличие сообщений.

```
while true do
 begin
  if PeekMessage(msg,0,0,0,PM_REMOVE)=false then
   begin
   // Для нас нет сообщений, и здесь мы можем
   // заниматься анимацией
   end
  else
   begin
    translatemessage(msg);
    dispatchmessage (msg);
   end;
 end;
```

Анимация



Теперь нужно написать логику движения самолета там, где я поставил комментарии в нашем новом обработчике событий. Напиши вместо комментариев следующее:

```
x:=x+1; //Увеличиваю позицию X самолета
if X-LastXState>10 then
begin
 State:=State+incparam; // Изменяю состояние
 if State=6 then // Если уже 6-е состояние, надо уменьшать
  incparam:=-1; // Приращение отрицательное
 if State=0 then // Если 0-е состояние, надо увеличивать
  incparam:=1; // Приращение положительное
 LastXState:=x; // Запомнить текущую позицию самолета
end;
SendMessage(Handle, WM_PAINT, 0, 0); // Перерисовать
```

Здесь в первой строке кода я увеличиваю значение переменной X на 1. После этого я проверяю, если переменная X - LastXState больше 10, значит самолет уже пролетел 10 пикселей, и можно менять его состояние (выводить следующий спрайт). Для этого я увеличиваю значение переменной State на значение, записанное в incparam. После этого проверяю состояние. Если переменная State равно 6, значит мы отображаем последний спрайт, и дальше некуда. Поэтому я изменяю приращение incparam на отрицательное, и в следующий раз переменная State будет уменьшаться. Ну а если State равна нулю, то приращение изменяю на положительное.

После изменения позиции самолета я отсылаю сообщение системе с помощью SendMessage, чтобы перерисовать экран. В качестве первого параметра я указываю указатель на мое окно, а второй - показывает тип сообщения (WM_PAINT - заставляет окно обновить свое содержимое).

Отображение

Математику анимации мы уже сделали, теперь нужно вывести на экран сам самолет в уже рассчитанную позицию. Функция вывода не изменилась, и мы будем использовать все ту же BltFast, но небольшая косметическая операция все же произойдет:

```
srcrect.Left:=0;
srcrect.Top:=State*90;
srcrect.Right:=180;
srcrect.Bottom:=State*90+90;
FBackgroundSurface.BltFast (X, Y, FTransImageSurface, @srcrect,
  DDBLTFAST_WAIT or DDBLTFAST_SRCCOLORKEY);
```

Вначале я заполняю структуру srcrect, которая будет указывать область, которую мы хотим скопировать. Так как у нас спрайты самолета выстроены в столбик, то левая и правая позиции неизменяемы - левая равна нулю, а правая равна 180.

Верх и низ области нужно рассчитывать, чтобы правильно вывести нужный спрайт в зависимости от состояния самолета. Высота каждого спрайта равна 90, значит верхняя позиция области копирования будет равна State*90, а нижняя еще на 90 пикселей больше. Все готово к отображению самолета, и можно вызывать функцию BltFast. В качестве первых двух параметров нужно только указать текущую позицию самолета - X и Y.



Рисунок 2. Наш летающий самолет

Disconnect

Как видишь, компьютерная анимация не так уж и сложна. Это только на первый взгляд требуются глубокие знания математики. Для реализации анимации на основе спрайтов мы обошлись только простыми операциями сложения, вычитания и умножения (даже деления, кажется, не было). Лично я пока не встречал в компьютерной графике ничего такого, что не укладывалось бы в школьный курс алгебры и геометрии. Конечно же, бывают сложные проекты, но большинство обходится школьным курсом.

Как всегда, исходники примера будут доступны на моем сайте www.cydsoft.com/vr-online после выхода этого номера в свет, а те, у кого нет Инета, могут найти их на нашем диске. Удачи!!!

P.S.У меня к тебе просьба, на сто баксов :). Не пиши мне большие письма. После появления рубрики «Кодинг» меня каждый день валят вопросами. Я не в состоянии всем рассказывать то, о чем пишут книги. Я могу что-то подсказать, где-то помочь, но не больше. А просьбы типа помоги написать прогу вообще нереальны. Я отвечаю только на те вопросы, где ответ займет несколько строчек. Целые лекции по мылу я разводить не могу. Я бы с удовольствием помог всем, но это НЕВОЗМОЖНО. Вас слишком много, а я один :(((. Поэтому лучше разбей свой вопрос на несколько маленьких и спрашивай постепенно, а не все сразу.





Сергей Овчинников



Игровые приставки

5 мифов, которые все еще вводят тебя в заблуждение



Ну вот, скажешь ты, опять вторгаются на нашу территорию. Исконную, писишную. Компутер - не тронь, он нам для дела нужен. Программировать, ломать, тексты набирать, в конце концов. Не надо лицемерия. Знаю я, для какого дела. Quake, Counterstrike, StarCraft, Baldur's Gate и прочая, и прочая. Как деловой инструмент компьютер, конечно же, незаменим. А вот в развлекательном качестве имеет массу достойных конкурентов. И главный из них - это многочисленные игровые приставки, которые устроены проще, стоят дешевле и, главное, при всем при этом, как правило, способны на большее. Именно поэтому практически все «прогрессивное человечество» предпочитает вкалывать за монитором, а расслабляться - с джойпадом у телеэкрана.

ENTER

В России игровые приставки почему-то считаются уделом младших школьников, а их имидж накрепко завязан на древнейших Dendy и Mega Drive, которые во всем мире были популярны в восьмидесятых и в самом начале девяностых годов. Что же касается игровых консолей нового поколения, начавших свое победное шествие по планете всего лишь год с небольшим тому назад, то вокруг них водят хороводы массы мифов, дать толкование которым меня и пригласили коллеги-хакеры. Предметом расследования станут три новейшие системы - Sony PlayStation 2, вышедшая в 2000 году, и чуть более новые Microsoft Xbox и Nintendo GameCube образца года 2001-го. Втроем они составляют основу гигантского рынка, обороты которого только в Америке составляют около 10 миллиардов долларов в год, больше, чем сборы всех американских кинотеатров. Так что игровые приставки и все, что с ними связано, - бизнес нешуточный. Трое конкурентов рассчитывают заполучить контроль над значительной его частью. Sony, стартовавшая годом раньше, пока демонстрирует полную решимость во второй раз подряд (после PlayStation) выйти из боя победителем.

Миф первый. Производительность и цена

Игровые приставки значительно дешевле компьютеров. Отсутствие монитора, ряда дорогих компонентов, массовое производство процессоров и материнских плат, памяти и аксессуаров, унифицированная архитектура - все это позволяет максимально удешевить готовую продукцию. При этом по техническим характеристикам игровые приставки ни в чем не уступают самым мощным PC, а по ряду параметров (например, по скорости обработки полигонной графики) серьезно вырываются вперед. Производителям игр также приходится ори-

Лучшие игры на приставках нового поколения:

1. Metal Gear Solid 2 (Konami, PS2) -
Атмосферный политизированный триллер.
2. Halo (Microsoft, Xbox) -
Неожиданно качественный представитель жанра FPS.
3. Pikmin (Nintendo, GC) -
Хитроумная и не в меру оригинальная стратегия.
4. Grand Theft Auto 3 (Rockstar, PS2) -
Криминальный автомобильный экшн на улицах мегаполиса.
5. Final Fantasy X (Square, PS2) -
Красивая, слезовыдавливающая RPG.
6. Super Smash Bros. Melee (Nintendo, GC) -
Бескомпромиссное мультяшное мочилово с героями всех нинтендовских игр.
7. Jet Set Radio Future (Sega, Xbox) -
Нон-стоп-скейт-стрит-графитти-экшн-под-убойный-саундтрек.
8. Jak & Daxter (Sony, PS2) -
Уникальный по красоте и насыщенности платформер от создателей Crash Bandicoot.
9. Gran Turismo 3 A-Spec (Sony, PS2) -
До предела навороченный автосимулятор.
10. Devil May Cry (Capcom, PS2) -
Модный, быстрый и хорошо стилизованный Resident Evil.

GAMECUBE, PLAYSTATION 2, XBOX: НАЧИНКА







	Xbox	GameCube	PlayStation 2
Центральный процессор	733 МГц Intel Pentium III	485 МГц IBM PowerPC «Gekko»	296 МГц Toshiba Emotion Engine
Графический процессор	233 МГц Nvidia GeForce 3	162 МГц ATI ArtX «Flipper»	150 МГц Sony Graphics Synthesizer
Оперативная память	64 MB унифицированной SDRAM PC100	43 MB MoSys 1T-SRAM	40 MB, в том числе 32 MB Rambus RDRAM
Звуковой процессор	100 Мгц Nvidia I/O + Sound	81 МГц Factor 5 Sound chip	33 МГц PSone I/O chip
Система кодирования 3D-звука	Dolby Digital 5.1	Dolby ProLogic II 5.1	Dolby Digital 5.1
Информационный носитель	DVD 4.7-8.5 GB	Matsushita mini-DVD 1.5 GB	DVD 4.7-8.5 GB
Проигрывание DVD-Video	Да, с дополнительным комплектом	Нет	Да
Проигрывание CD-Audio	Да	Нет	Да
Жесткий диск	Да, 8-10 GB (как повезет ;-)	Нет	Дополнительно, 40 GB
Модем/сетевая карта	Нет/Да, 10/100	Пока не доступны	Да/Да, дополнительно
Memory Card	8 MB	0.5 MB	8 MB
Вес	4.5 Кг	1.5 Кг	3 Кг
Дата выхода в США	15.11.2001	18.11.2001	26.10.2000
Дата выхода в Японии	22.02.2002	14.09.2001	04.03.2000
Дата выхода в Европе	15.03.2002	03.05.2002	27.11.2000
Цена в США	$299	$199	$299
Цена в Японии	34.800 иен	25.000 иен	29.800 иен
Цена в Европе	479 евро, 299 фунтов стерлингов	299 евро	399 евро
Количество доступных в день премьеры игр	19	12	33

Самые перспективные проекты Nintendo GameCube

1. Metroid Prime (Nintendo/Retro Studios), ноябрь 2002
Суровые жизненные реалии, определяющие развитие игровой индустрии, заставили Nintendo несколько изменить своему вечному детсадовскому имиджу. Поскольку даже на игровых приставках все большую популярность приобретают игры кровавые и жестокие, ветерану индустрии пришлось покопаться в закромах и оживить суперпопулярный в начале девяностых сериал Metroid, хорошо укладывающийся в современную концепцию «максимум насилия». Metroid Prime, новая игра, разрабатываемая эксклюзивно для GameCube, обещает стать настоящим раем для всех любителей FPS. Nintendo, правда, не спешит отнести игру к этому известному жанру и предпочитает называть ее «exploration action». Так или иначе, вжившись в образ бронированной супергероини Samus, вам придется исследовать инопланетные миры, кишащие всевозможными формами жизни, бороться с кибернетическими монстрами и активно использовать разнообразные гэджеты. Meroid Prime непременно станет одним из главных хитов этой осени и добавит Nintendo очков в непростой борьбе с Sony и Microsoft.

2. Mario Sunshine (Nintendo/Nintendo EAD), август 2002
Занимаясь такими «продвинутыми» проектами, как Metroid, Nintendo не забывает и о тех играх, которые сделали предыдущие платформы компании столь популярными. В послужных списках Nintendo игры сериала Mario занимают особое место. Перефразируя классиков, можно смело заявить: «Марио - это наше все!». Новая игра сериала - уже седьмая по счету, работа над ней идет с конца 1998 года - обещает в очередной раз вывести платформенный жанр на новый уровень. Как всегда, отличная графика, потрясающий дизайн с живыми, постоянно изменяющимися уровнями, некоторые новые «фишки» в игровом процессе. Например, специальная водяная пушка, которую Марио таскает на спине на манер рюкзака и при помощи которой смывает капли краски, что под действием жаркого солнца льется прямо с неба. Графика Mario Sunshine пока что не приводит в щенячий восторг, но к моменту релиза эти сдержанные эмоции наверняка трансформируются во что-то более радостное.

3. Legend of Zelda (Nintendo/Nintendo EAD), зима 2002-2003
Еще один «легендарный» представитель традиционной игровой библиотеки от Nintendo. Сериал, повествующий о приключениях юного эльфоподобного героя по имени Линк, был рожден еще в середине восьмидесятых и с тех пор выход новых серий осуществляется регулярно, раз в два-три года. В отличие от Mario, Legend of Zelda куда более серьезно ориентирована на сюжетное повествование. Тут есть и выразительные персонажи, и хорошо очерченные характеры, но нет массы текста, тучи параметров и прочих ролевых закосов. В новой игре Линк предстанет перед игроками совсем юным, а графика очередной Zelda больше похожа на яркий мультфильм, нежели на массу собранных из полигонов конструкций. Несмотря на детский облик проекта, опыт показывает, что от этого Zelda, возможно, теряет в имидже, но отнюдь не в качестве. Невероятное качество проработки игрового процесса и отлично смоделированные подземелья всегда заставляли игроков от мала до велика ночами просиживать за экраном. Сел поиграть на полчасика, очнулся - а на дворе уже утро.

Сергей Овчинников

ентироваться на конечную конфигурацию, а не на широкий спектр машин с разными процессорами и разными графическими платами - в результате производительность удается оптимизировать самым лучшим образом. Кроме того, в отличие от производителей компьютерного железа, создатели игровых приставок не ставят себе целью получить прибыль с каждой проданной коробочки. Напротив, они обычно продают приставки с небольшим убытком (так, например, себестоимость каждого Xbox составляет порядка 420 долларов, а продается приставка всего за 300), рассчитывая вернуть деньги на продаже самих игр. Такая схема ведения бизнеса существует уже около двадцати лет, полностью устраивая как бизнесменов, так и покупателей. Так что ценник с привлекательными цифрами - еще не повод для оценки возможностей. Коньюнктура рынка - вот важнейший показатель.

Миф второй. Универсальность

На игровых приставках можно играть. Этот факт бесспорен. А вот способны ли они на что-то, не совсем связанное с интерактивными развлечениями? Например, на компьютере можно слушать музыкальные диски, смотреть VideoCD и DVD, работать в Интернете. Возможности игровых приставок по этой части зависят от философии производителя. Так, например, компания Nintendo считает, что, кроме своей основной задачи, приставка не должна делать больше ничего и не надо морочить людям головы. Они покупают GameCube, чтобы играть, - вот пусть и играют. У Sony и Microsoft идейные установки другие. Эти производители предпочитают универсальность. И PlayStation 2, и Xbox с легкостью проигрывают музыкальные диски, на них можно смотреть фильмы со вполне приличным качеством бытового DVD-плеера. В Xbox также встроен сетевой адаптер, позволяющий выходить в Интернет. В первую очередь - для онлайновых игр, но простенький браузер наверняка тоже будет. Единственная загвоздка - о времени введения в строй своей сетевой службы компания пока не сообщает. У Sony с этим дела немного лучше - служба заработает уже этим летом. Но для того, чтобы получить возможность выходить в Сеть, владельцам PS2 придется докупить модем и жесткий диск, которые обойдутся примерно в $100-150.

Миф третий. Дороговизна игр

Не секрет, что большая часть отечественных PC-игроков предпочитает пользоваться пиратской продукцией, лишь изредка (и по случайности) выбирая дешевые лицензионные локализации от компаний «1С», «Руссобит» или «Бука». Для новых игровых консолей пиратский рынок пока еще не развит. Лицензионные игры, привезенные из Америки, стоят в магазинах и в Интернете порядка 70 долларов ($50 американской розницы плюс расходы по доставке и наценка), что для большинства игроков является суммой совершенно неприемлемой. С европейскими версиями дело обстоит куда лучше. Поскольку Россия худо-бедно, но все же входит в рамки понятия «Европа», то российским компаниям разрешается



Самые перспективные проекты Microsoft Xbox

1. Project EGO (Microsoft/Lionhead), зима 2002-2003

Студия Lionhead, возглавляемая автором таких проектов-монстров, как Populous и Dungeon Keeper, продолжает покорять горизонты человеческого сознания и восприятия. После того, как нам предложили побыть по очереди божеством (Populous), владельцем мрачного подземелья (DK) и воспитателем безмозглого монстра (Black & White), пришел черед чего-то более ответственного и интересного. Как насчет того, чтобы взять на себя ответственность за одну человеческую жизнь и прожить ее вместе со своим героем в романтическом фэнтезийном мире? Вам подсовывают не какой-нибудь Diablo или низкосортную RPG. В Project EGO нет сюжета, нет единственно верного пути, нет подсказок и напутствий. Есть только гигантский мир, полный возможностей, самых непредсказуемых событий и невероятных ситуаций, многие из которых смоделированы не разработчиками проекта, а действиями самих игроков. Ваш герой путешествует по этому необычному миру, взрослеет, учится, сражается, возможно, торгует, колдует или ворует, изменяется сам и изменяет все вокруг себя. Обещанный масштаб игры и ее разнообразие пока просто не укладываются в голове. С другой стороны, то же самое имело место и в случае с Black & White. Посмотрим, каков окажется результат на этот раз. Правда, придется подождать - не исключено, что дата выхода игры будет отложена, и не раз.

2. GUNVALKYRIE (Sega/Smilebit), весна 2002

Компания Sega, лишившаяся собственной игровой платформы, активно поддерживает всех лидеров рынка, но к Microsoft у нее отношение особое. Хотя бы потому, что с этой компанией Sega конкурировать еще не приходилось, оттого и дружба. К раннему проекту Jet Set Radio Future уже совсем скоро присоединится и еще один, от той же команды разработчиков. Действие GUNVALKYRIE (проект при всякой возможности пытается показать, что он является игрой с большой буквы) происходит в параллельной Вселенной, в которой человечество, воодушевленное техническим прогрессом, занялось исследованием космоса не в конце двадцатого века, как мы, а уже в девятнадцатом. Космические корабли с чугуниевым литьем, фраки, смокинги, цилиндры, бластеры, ракеты, лазерные пушки. Не правда ли, увлекательное сочетание? Разумеется, будут и злодеи для начинки двух десятков гигантских уровней - инопланетные монстры, по виду весьма напоминающие жуков и тараканов из верховенских Starship Troopers. Действие демонстрируется от третьего лица, камера свободная (временами даже чересчур). Акробатические прыжки сочетаются с тяжелой огневой мощью. В результате на экране творится такое, что престарелым бабушкам играть не рекомендуется. Разве что продвинутым…

3. Rallisport Challenge (Microsoft), весна 2002

Microsoft пока лучше своих конкурентов справляется с неизбежным «спадом после премьеры», обычно сопровождающимся снижением темпов выпуска новых игр на платформу и непременным падением их качества. У Xbox почему-то такой проблемы не наблюдается, и новые вполне интересные проекты появляются ежемесячно. Причем все они постепенно и методично закрывают пустующие жанровые ниши, делая приставку от Microsoft все более и более привлекательной в глазах покупателей. «Окошко» с подписью «Реалистичный раллийный симулятор» было решено закрыть перспективной разработкой под названием Rallisport Challenge, которая хоть и не несет на себе торговой марки известного гонщика или лицензии от FIA, но обладает рядом качеств, позволяющих простить проекту эти прегрешения. Потрясающее качество графики бросается в глаза даже при просмотре скриншотов. Еще очевиднее технические преимущества Xbox становятся при личном знакомстве. Все необходимые эффекты, отличные модели автомобилей (12 тысяч полигонов на каждый), отражения, свет, елочки и березки - все это производит отличное впечатление. Но окончательно добивают газоны, в которых каждая травинка прорисована отдельно. Удачная модель управления (не симулятор, но и не простецкая аркада) и хороший дизайн трасс не оставляют сомнений. Это лучшая раллийная гонка на сегодняшний день.

Самые перспективные проекты Sony PlayStation2

1. Final Fantasy XI Online (Square), осень 2002

Уже ближайшим летом игровая приставка Sony совершит первые шаги на принадлежавшей некогда исключительно PC территории. Dreamcast при всей своей инновационности не смог пробить даже маленькой бреши на рынке сетевых игр. У Sony ресурсов объективно побольше. Одним из главных ударов компании станет созданная издательством Square одиннадцатая игра сериала Final Fantasy, специально для которой создана игровая служба PlayOnline. Final Fantasy XI, на первый взгляд, является вполне стандартной MMORPG, инспирированной такими творениями, как Ultima Online и Everquest. Так-то оно так, да не совсем. В творении Square весьма замысловатым образом сочетаются как элементы вышеназванных проектов, так и собственные идеи. Отличия - в отношении к сюжетной линии, в представлении классов героев, в механике боя. Плюс, разумеется, в FFXI значительно лучше графика. К концу года игра также теоретически должна выйти на PC, тем самым значительно пополнив список своих поклонников. В целом, приставочные сетевые RPG пока почти ничем не отличаются от PC'шных. Привнесут ли японцы что-то новое в устоявшийся жанр, покажет время.

2. Xenosaga. Episode 1: Der Wille Zur Macht (Namco/MonolithSoft), осень 2002

Еще один представитель ролевого жанра, но куда более экстравагантный и необыкновенный. Традиционные японские RPG, как известно, далеки по концепции и смысловому наполнению от своих американских и европейских собратьев. Настоящая японская RPG создается не для красивой боевой системы и комплексных характеристик. Она должна рассказывать историю, часто довольно традиционную, но зато с непременным раскрытием характеров всех без исключения героев (которых в средней JRPG бывает несколько десятков), массой философского подтекста и жизнеутверждающей фабулой. Так вот, даже по меркам японских RPG Xenosaga - явление совершенно уникальное. Прозванная своими создателями «космической» оперой, игра переносит нас на несколько тысяч лет в будущее, где разыгрывается трогательная и увлекательная история с глубоким эмоциональным, религиозным и философским загрузом. По степени воздействия и качеству «погружения» я бы сравнил этот проект с книгами серии «Дюна» Фрэнка Херберта. Такие же неординарные типажи героев, глобальные безумства, размышления о роли религии в человеческом обществе, о войне миров, о силе и слабости отдельной личности на вселенском уровне и так далее, и так далее. Внешней оболочкой этого ужаса служит вполне симпатичная высокотехнологичная игра, английский перевод которой появится на прилавках уже этой осенью. Берегитесь!

3. Tekken 4 (Namco), лето 2002

Четвертая серия прославленного файтинга появилась в залах игровых автоматов еще в августе прошлого года. Тогда Tekken с готовностью подтвердил свой статус суперхита, лишь немного уступив более раскрученному в Японии Virtua Fighter 4. В конце марта японцы, а к лету и все остальные владельцы PS2, получат возможность сыграть в Tekken 4 и в домашней обстановке. В отличие от «переходного» и, чего уж скрывать, весьма посредственного Tekken Tag Tournament, четвертый Tekken представляет на суд игроков несколько измененную игровую систему. Поединки теперь проходят на полностью трехмерных интерактивных аренах, вписанных в неровные ландшафты. По этим аренам можно свободно передвигаться, а конструктивные их особенности использовать в тактике боя. Нет ничего проще, чем зажать противника в углу и дубасить его что есть силы об острые края каменной статуи. Графически проект хорош, но далек от идеала. Качество «отделки» персонажей не вполне соответствует требованиям нового поколения консолей, анимация выглядит не слишком убедительно. Но зато в наличии яркие цвета, вполне качественные текстуры, масса симпатичных эффектов и убедительные игровые арены.



поставлять в страну игры и приставки почти официально. Так, например, компания «СофтКлаб» является дистрибьютором игровой продукции таких известных издательств, как Sony, Electronic Arts и Infogrames. Их приставочные проекты приходят к нам по другим ценам, позволяющим в рознице установить планку в 1500-1800 рублей за игру, что уже совсем неплохо. В этом плане особенно хороши перспективы европейской версии PlayStation 2 - не исключено скорое появление полностью локализованных проектов, которые будут продаваться по уж совсем демократичным ценам. Однако европейский игровой рынок куда инерционнее американского, да и выход новинок часто запаздывает. Так что тем игрокам, которым нужно быть в курсе всех премьер, придется все же разоряться на американские версии всех приставок.

Миф четвертый. Модификация

Изменить в конструкции игровой консоли практически ничего невозможно. Лишь в редких случаях производители приставок позволяют пользователям прикупить какие-нибудь расширения, позволяющие улучшить технические характеристики машины. Впрочем, эта практика, как показал горький опыт многих производителей, до добра не доводит. Новое расширение покупают далеко не все, парк систем разделяется, люди начинают путаться, разработчики паниковать, а продавцы - убирать продукцию компании с магазинных полок. Так что ни о каком апгрейде речи идти не может. Это и хорошо, и плохо. Хорошо - потому что не придется разоряться на модернизацию. Плохо - потому что по прошествии четырех-пяти лет приставка попросту устареет и отправится на чердак/помойку (нужное подчеркнуть). Единственное, что можно изменить в игровой приставке, это ее региональные аппетиты. Производители консолей, как правило, делают системы, созданные для разных рынков (американского, японского, европейского), несовместимыми друг с другом, чтобы можно было всегда держать в руках все рычаги влияния на рынок и в конечном счете больше зарабатывать. Вот как раз эта защита часто легко снимается. Так, у GameCube достаточно лишь подвести к одному из гнезд на материнской плате пару проводов и переключатель. Для PlayStaion 2 умельцы полулегально делают многочисленные чипы с двадцатью-тридцатью проводами для пайки. Эти чипы зачастую позволяют не только снять региональную защиту, но и проигрывать «резервные копии» - именно за это Sony нещадно преследует всех производителей такой продукции. Что касается Xbox, то японская премьера приставки состоялась совсем недавно, а европейская ожидается на днях, так что актуальная проблема пока не решена. Но наверняка будет решена совсем скоро.

Миф пятый. XXX-битные приставки

Игровые приставки древности (80-х и начала 90-х годов) классифицировались таким понятием, как «битность», которая зависела от разрядности центрального процессора консоли. До сих пор многие игроки всерьез воспринимают такую классификацию и активно спорят друг с другом, сколько бит в какой из консолей и какая из них в результате получается мощнее. Сегодня термин практически полностью потерял свою значимость. Сверхмощные процессоры Pentium (сидящие внутри Xbox) до сих пор технически являются 32-битными, а консоли нового поколения GameCube и PlayStation 2 построены на базе 64-битных процессоров, хотя сами приставки гордо называют себя 128-битными. Сегодня на это уже не стоит обращать внимание. Куда важнее архитектура процессора и его финальная производительность.

EXIT

Polosatiy (polostiy@cyberfight.ru)

Дневник Полосатого

В начале июля в Париже прошел один из самых ожидаемых турниров по Quake3 и Counter-Strike - Lan Arena 7. Впервые за долгое время европейский турнир посетила американская команда.

ENTER

Пусть даже одна, но по крайней мере теперь можно сравнивать уровень игры европейцев и игроков из-за океана. Ну а этой единственной командой стал Q3 клан 519 - сильнейший на данный момент в Америке, и именно ему предстояло защищать честь своего континента. Всего в турнире принимало участие 16 команд по Q3 и 16 - по Counter-Strike. Россию на турнире представлял клан ForZe, который еще не успел остыть от блистательного выступления в Кельне (Германия), где ForZe выиграли турнир CPL Europe. Но в этот раз конкурентов было в несколько раз больше, ведь многие понимали, что Lan Arena 7 - один из последних крупных тимплейных турниров по Q3, поэтому все команды готовились очень серьезно. Соревнования по обеим играм начинались по групповой системе (4 группы по 4 команды). К ForZe в группу попали 3 европейские команды - aAa, Vikings и Shuuk. Первый матч наши играли против немцев из Shuuk и выиграли со счетом 2:0 по картам (112:92 на q3dm14, 129:106 на ospdm5). Одновременно с этим американцы из 519 проиграли на двух картах с крупным счетом шведам из Eyeballers. Во втором круге ForZe играли с хозяевами соревнований, лучшим кланом Франции Against All Authority. В прошлом году я сам выступал за aAa, в общем, ребята они неплохие :p, что впрочем не помогло им. ForZe выиграли карту q3dm14 со счетом 141:111, после чего французы раскисли и проиграли

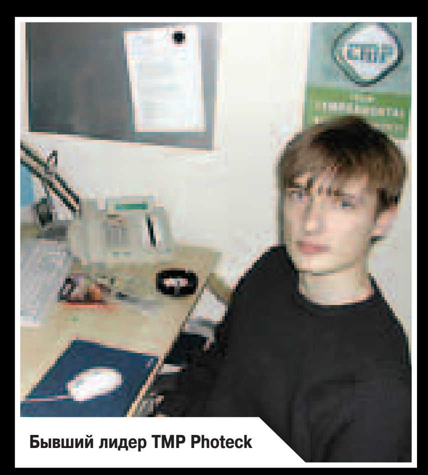
Из-за нелепой ситуации, возникшей с русской командой, ForZe проиграли и упали в лузера.


Клан 519


Zero4 из клана 519

Клановые новости. За последний месяц сразу несколько кланов потеряли или приобрели новых игроков. Вообще, понятие клана несет в себе эдакий образ одной тусовки, семьи, но в данном случае геймеры находятся на перепутье. Ведь эпоха Quake3 и Counter-Strike потихоньку идет к концу, и в скором времени народ начнет играть в новые игры. Такие, как Doom3, UT2003 и другие. Пока есть немного информации о третьем Думе, но и этого хватает для того, чтобы народ начало колбасить. Вследствие чего и происходят метания из клана в клан. Теперь подробнее.

Tempramental. В команде происходит полная неразбериха, но в отличие от ситуации с c58, клан TMP покинули не игроки, а руководство. TMP-Photeck, создавший и продвигающий развитие команды в течение долгого времени, ушел из команды. Насчет игроков ничего не ясно, у команды есть два состава, но будущее не ясно.


Бывший лидер TMP Photeck

Завершился популярный онлайн-турнир Clanbase Quake3 Nations cup. Своеобразный чемпионат Европы, но только по Интернету. В турнире принимали участие 19 национальных сборных команд, три из которых были отсеяны в самом начале игр. Соревнования проходили по схеме 4 группы по 4 команды в каждой. В плей-офф выходят 2 команды, и так до финала. Сборную России на турнире представляли Pow3r, Mikes, ShadZy и Polosatiy, то есть я :P.
В своей группе мы обыграли Норвегию (123-79 на cpm4, 115-92 на q3dm14), Финляндию (104-64 на ospdm5, 99-125 на q3dm14, 125-96 на ospdm6) и проиграли Швеции (техническое поражение).
В 1/4 финала мы довольно легко обыграли бельгийцев со счетом 3:0, правда, сказалось то, что у нас был меньший пинг (все-таки игра по Интернету). Счета были такими: 158-82 на ospdm5, 124-74 на q3dm14, 147-120 на cpm4.
Полуфинал против Германии - одной из сильнейших европейских команд. Мы очень ответственно подошли к этой игре, хотя тренировались немного. Мы очень долго искали сервер для игры, подходящий для обеих команд. В итоге получилось, что у нас было некоторое преимущество в пингах, но времени для поисков уже не было, и мы начали игру. Первая карта - q3dm14. С самого начала игры немцы заняли контроль на уровне и повели в счете. К пятой минуте мы проигрывали фрагов 25, но затем смогли перехватить инициативу и не отпускали ее до конца матча. Финальный счет - 81-63 в нашу пользу. Вторая карта - снова q3dm14. Так уж получилось, что обе команды выбрали эту карту, и у нас уже было психологическое преимущество после победы в первом матче. Вторая игра получилась менее напряженной, о чем и свидетельствует финальный счет - 102-83. Третья карта - ospdm5 (выбор немцев). В этом матче наш пинг был очень нестабилен, и всю игру мы проигрывали. В общей сложности на паузы в игре ушло более 20 минут - настолько часто у нас пинг подскакивал до 200 миллисекунд. За минуту до конца мы проигрывали 10 фрагов, но сумели собрать последние силы и победить - 75-73, и мы в финале, где нас уже ждала шведская сборная.
Финал против Швеции. К сожалению, полноценного финала не получилось, так как опять подвел нестабильный Интернет. В столь ответственном матче у команды просто опустились руки, и мы проиграли с крупным счетом.
Я хотел бы поблагодарить интернет-кафе АСВТ за предоставленную возможность принимать участие в онлайн-турнирах. Хотя и были случаи, когда пинг подводил нас, но в целом все прошло гладко, и мы надеемся в будущем улучшить наши результаты.

Cyberfight. Команду покинули два основных игрока - ShadZy и noBap. Причин много, но основная из них - команда изжила себя. Мы отыграли все возможные турниры, и было непонятно, что ждет команду впереди. noBap перешел в клан ForZe к своему другу uNkind'y, а вслед за ним ушел ShadZy. Возможно, c58 сделает новую команду для игр 4x4, но пока что все только в планах.


Team C58


QPO - вид со спины

cpm4 с очень крупным счетом. Клан 519 в этот момент встречался с английским кланом 4Kings, этот матч завершился вничью (1:1 по картам). Третий матч у ForZe был против серебряных призеров Euro Cup 5 - датского клана Vikings. Это был очень напряженный матч, и хотя ForZe выиграли выбранную им карту q3dm14 (92:54), во втором матче они все-таки уступили. Пусть даже на один фраг (106:107 на cpm4), но это поражение стало первым звонком. Таким образом матч между ForZe и Vikings завершился вничью, и обе команды прошли в следующий круг (Vikings до этой встречи также выиграли все свои матчи). А вот клан 519, к сожалению, после своей третьей игры покинул турнир. Безликая игра против немцев из mTw, и разочарование для всех американских болельщиков.

Второй раунд турнира представлял собой ставшую уже классической систему Double Elimination, т.е. на выбывание, но с правом команды проиграть одну встречу.

В 1/4 финала ForZe должны были встречаться с командой iCE cLIMBERS, у которых они выиграли в финале CPL Cologne. Но из-за нелепой ситуации, возникшей с русской командой, ForZe проиграли и упали в лузера. А случилось следующее. ForZe по непонятным причинам опоздали на второй день соревнований и получили техническое поражение на первой карте, что, несомненно, выбило команду из колеи. Вторую карту (q3dm14) они уступили со счетом 100-108.

Первым соперником ForZe в лузерах стал клан Regeneration - уверенная победа наших 2:0 (174-107 на cpm4, 153:136 на ospdm5). Ну а дальше случилось то, чего многие ожидали. Хотя и создалось впечатление, что ForZe начали набирать обороты, но клан Vikings, с которыми наши сыграли вничью в первом раунде, остановил русских игроков, и ForZe покинули турнир, разделив 5-6 места с кланом Eyeballers. Счета игры ForZe против Vikings - 114:138 на ospdm5, 80:77 на q3dm14, 97:106 на cpm4.

Турнир тем временем продолжался. Полуфиналы: IC против mTw - 2:1 (161:82 на cpm4, 114:129 на q3dm14, 115:97 на ospdm5); QPO против Vikings - 2:0 (92:69 на ospdm5, 85:72 на q3dm14). В финале виннеров встретились QPO и iCE cLIMBERS. Фактически победитель этой встречи становился победителем турнира. Этой командой стал клан QPO, а IC упали в лузера (147:143 на cpm4, 122:97 на ospdm5). После этого IC в финале лузеров снова встретились с mTw и победили со счетом 2:1 (109:95 на cpm4, 97:127 на q3dm14, 124:92 на ospdm5).

Суперфинал. QPO против IC. Две самые аркадные команды Европы и две разных шведских школы. IC было необходимо для победы выиграть на четырех картах подряд. И они почти сделали это, но QPO собрались в самый ответственный момент и стали европейскими чемпионами. Чтобы выявить победителя, пришлось QPO и IC играть целых пять карт: (133:137 на cpm4, 96:108 на ospdm5, 104:143 на cpm4, 154:123 на ospdm5, 142:102 на q3dm14). Финальная расстановка команд:

1 место - QPO (Seka, Senti, proZac, Hjalmarzka, Tech) - 5.600 евро.
2 место - iCE cLIMBERS (Toxic, Gopher, Belth, Panicore, Phantom) - 2.800 евро.
3 место - mTw (Slinger, Neok, ZyZ, Willow) - 1.400 евро.

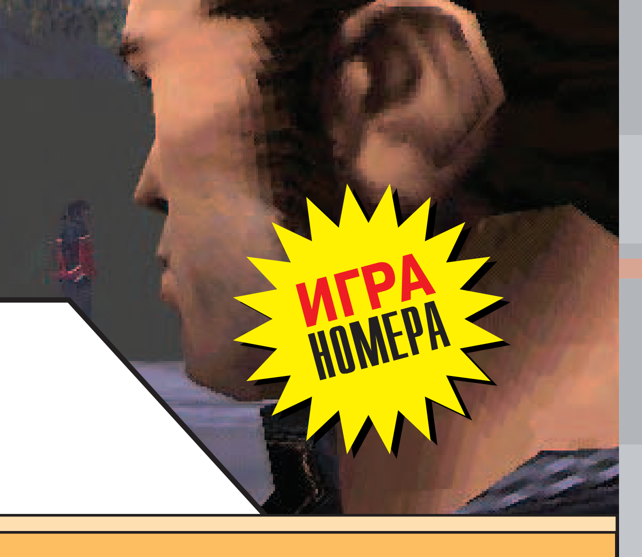
Результаты турнира по Counter-Strike 5x5 в рамках Lan Arena 7:
1 место - mTw.alternate - 7.000 евро.
2 место - Ice-2easy - 3.500 евро.
3 место - Infernum - 1.750 евро.

Чтобы выявить победителя, пришлось QPO и IC играть целых пять карт.

ForZe. Команда пополнилась сильными московскими игроками. Из c58 в ForZe перешли ShadZy и noBap, а из TMP - FunT. В целом ситуация очень плохо скажется на командной игре в России. У ForZe просто не осталось конкурентов, и смысл в турнирах пропадает. Хотя, возможно, волна новых талантливых игроков спасет ситуацию, но придется подождать, а там уже и новая игра не за горами.

EXIT

p0r0h (p0r0h@real.xakep.ru)



GTA3: Руководство анархиста
Настройка, секреты, фишки

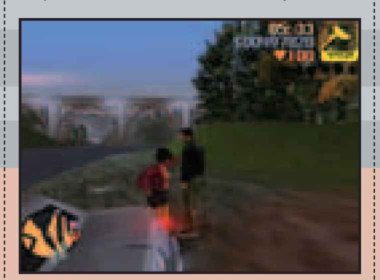
ENTER

Как все начиналось…

В сети появились слухи о скором появлении долгожданного GTA3. Ждем-с. У буржуев игра уже появилась, и они, как и полагается, писают кипятком от восторга. Однако вместе с восхищением начинают литься периодические сопли о странных тормозах даже на крутых тачках. Хех, и не такое видали… Вторую ночь усиленно, но неторопливо закачиваются байтики хакнутого дистрибутива. И, наконец, игра проинсталлена! Понеслось…

Боремся с тормозами

Как известно, GTA3 довольно требовательна к ресурсам, но иногда умудряется тормозить даже на неслабых компах. Так вот, чтобы эти долбанные тормоза тебя не доставали, скачай программку 3d-Analyze (линк на врезке). Она позволяет вполне нормально



играть даже с видюхами класса GeForce 2 MX (правда, проц должен быть довольно шустрый). Для этого запускай ее, в разделе «EXE» жми «Select» и выбирай екзешник с игрой (что-нибудь типа GTA3.exe :)), аналогично в «DLL Path», только на этот раз кликай на mss32.dll. Теперь только требуется в опциях DirectX 8.1 выставить галочку напротив «force SW TnL», нажать RUN и наслаждаться жизнью :]. Еще в БИОСе будет не лишним поставить по минимуму размер appertura size. Также полезно произвести дефрагментацию диска и установить фиксированный размер файла подкачки (мегов на 100-200). Теперь все должно если не летать, то уж не ползать точно…

Заливаем свой музон

Для того чтобы во время беспредела на дорогах слушать по радио свои любимые трэки, скопируй их в папку «mp3» в каталоге с проинсталленной игрой (после патча проигрывать mp3 трэки можно из любой папки на винте - прим. Ядовитого). Теперь, когда будешь кататься на точилах, можешь, как обычно, переключать радио, но уже к списку радиостанций добавился твой «мп3 плейер» с убойным музоном ;].



Снимаем проститутку

А почему бы и нет? Тем более, в представительницах столь древней профессии на улицах городов GTA3 дефицита не наблюдается. Однако в процессе съема проститутки есть свои хитрости и нюансы. Для начала нужно угнать подходящую тачку, т.к. от спецмашин типа «скорой помощи», такси и полиции они предпочитают держаться подальше. Затем, заметив продажную тетку, подъезжай к ней, тормози и жди, пока она наклонится к окну твоей точилы и начнет обсуждать детали предоставления своих сексуальных услуг :]. После непродолжительного разговора и взаимного согласия вези ее в какое-нибудь безлюдное место и наблюдай за процессом… Помимо эстетического удовольствия ты можешь существенно поправить свое пошатнувшееся здоровье (вплоть до 125%). Ну, а если начнет душить жаба из-за потраченного бабла, смело мочи ее после полового акта и забирай свои буказоиды.

В процессе съема проститутки есть свои хитрости и нюансы.



Апокалипсис в городе

Для полного дестроя нужно, чтобы были доступны все три города. Тогда можно смело начинать свое черное дело. Убийство, второе, третье, сбитые пешеходы, расстрелянные ублюдки в форме - не останавливайся! Чувствуешь привкус крови во рту? Отлично! Мочи их всех! Загораются «звездочки», и копы с ФБРовцами устроили за тобой погоню, как за Усама Бен Ладеном? ОК, это только тебе и нужно! Продолжай беспощадную бойню. Как только загорятся все шесть «звезд» и от пота начнет заклинивать мышку и клаву, высшие силы пошлют для тебя настоящий ТАНК прямо с неба! Представляешь, что можно натворить с такой машиной для убийства и твоим воспаленным мозгом ;]? Если хочешь продолжить дестрой после перекура, загони танк в свой гараж и сохраняйся - при следующей загрузке он будет ждать тебя в гараже ;].

3d-Analyze
http://www.tommti-systems.de/start.html

Эта прога поможет тебе вылечить глюкавую тормознутость GTA3, да и вообще - полезная утилка.

Расстрел пешеходов

Пеших (и ездячих :)) можно мочить и из тачки. Для этого бери УЗИ и нажимай кнопку боковой стрельбы («1» или «2» на стандартном управлении и «Q» или «E» на классическом). Это особенно эффективно в районах с враждебными бандами, да и мочкануть бегущего к тачке копа тоже прикольно ;].







Затариваемся пушками

Без оружия в наше время никуда. Особенно в городах GTA3. Вот только каждый раз мотаться в оружейный магазин, чтобы вооружиться до зубов, несколько обломно, да и де-

За каждую убитую тачку дают 1000 буказоидов, но удовольствия от суицидной езды неизмеримо больше ;].

нег уходит прилично (лучше приберечь их на проститутов :)). Однако эта проблема легко устраняется. Ты наверняка находил где-нибудь секретный сверток. Так вот, если собрать десять таких пакетиков, то у тебя в логове появится пистолет, если двадцать - УЗИ и т.д. (ну, а если найдешь все сто, то дадут много зеленых бабок и базуку ;)). Радует то, что пушки всегда будут находиться около твоего дома, вожделая свежей крови.

Свой среди чужих

Ты уже, наверно, заметил, что когда угоняешь какую-нибудь спецмашину типа «скорой» или такси, тебе предлагают поработать на ней. Так вот - работа, конечно, полный отстой, по определению, но и от нее можно получить реальную пользу. Например, если, управляя ментовской тачкой, замочить десять бандюг, то в твоем логове появится полицейский значок (если еще десять, то уже два значка - простая арифметика :)). Однако и здесь есть своя фишка - если во время преследования «криминала» нажать «Esc» (затем снова вернуться), когда он находится в зоне видимости, то бандюган остановится, выйдет из машины, и уже тогда его можно спокойно переехать. Согласись, это гораздо проще, чем гоняться за ними по всему городу :]. Аналогичную процедуру можно проделать и на «скорой». И, как ты уже догадался, в логове будет здоровье. Для этого нужно спасти 40 доходяг. Ну, а если продолжить и дальше свою святую миссию, то дома можно обнаружить уже адреналиновую таблеточку ;]. Играя за пожарных и потушив на каждом острове по 20 тачек, ты получишь, как ни странно, огнемет. Что еще можно поиметь? Например, секретную тачку - Borgnine Taxi. Для этого нужно обслужить на такси 100 пеших лошков. Машинка эта, кстати, появляется на стоянке такси в Portland'е (хинт, чтобы искать не замучался ;)).

Миникамикадзе

Хочешь покататься на взрывающихся микромашинках? ОК, тогда ищи специальный синий фургон. Если искать напрягает, то подсказываю - в первом городе он находится около заправки, во втором - около казино, в третьем - возле твоего логова. Когда ты, наконец, доберешься до



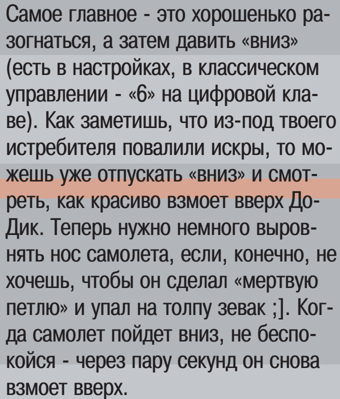
Бандюган остановится, выйдет из машины, и уже тогда его можно спокойно переехать.

этого фургона и заберешься в его фургонистое чрево, ты получишь задание замочить тачки какой-нибудь банды. Только мочить их придется как раз на радиоуправляемых машинках, начиненных взрывчаткой. За каждую убитую тачку дают 1000 буказоидов, но удовольствия от суицидной езды неизмеримо больше ;].

Полеты во сне и наяву

Признайся, ты всегда хотел летать? Я тоже. И до сих пор летаю... Во сне :]. В GTA3 тоже можно полетать всласть. Для этого нужно, чтобы был открыт третий город. Собственно, там и находится аэропорт, а в нем можно разыскать маленький самолет DODO.

Однако просто сесть и сразу же полететь не получится. Тут нужна особая сноровка и технология полета.

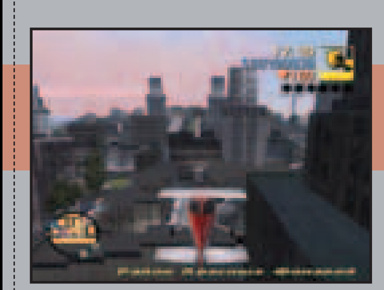


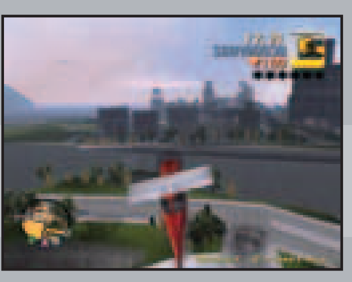
Самое главное - это хорошенько разогнаться, а затем давить «вниз» (есть в настройках, в классическом управлении - «6» на цифровой клаве). Как заметишь, что из-под твоего истребителя повалили искры, то можешь уже отпускать «вниз» и смотреть, как красиво взмоет вверх ДоДик. Теперь нужно немного выровнять нос самолета, если, конечно, не хочешь, чтобы он сделал «мертвую петлю» и упал на толпу зевак ;]. Когда самолет пойдет вниз, не беспокойся - через пару секунд он снова взмоет вверх.

Таким образом можно довольно долго летать и наблюдать жизнь города со всеми его тайными, не очень тайными и совсем не тайными местами (например, стадионом ;)). Приобретя необходимую сноровку, загоняй ДоДо в гараж во втором городе, чтобы потом каждый раз не мотаться в аэропорт.

Танковое безумие

Оказывается, летать можно не только на маленьком ДоДике, но и на танке! Представляешь, как летают танки? Я тоже не представлял, пока однажды мне не удалось каким-то непостижимым образом на нем взлететь. Для этого нужно всего лишь найти длинный прямой участок, развернуть танк (чтобы он ехал задом) и одновременно с разгоном быстро и бесперебойно начать палить из пушки. Танк начнет взвывать и все больше набирать скорость, пока, наконец, не взлетит, заставляя пешеходов в быстром темпе расслаблять прямую кишку ;].





Как все закончилось...

Режущий слух скрип открывающейся двери. Странно улыбающиеся люди в белом. Мозг активно пытается сопротивляться, но обмякшее тело никак не реагирует. Самый длинный с заметной сутулостью приближается все ближе и ближе. У него что-то в руке, и он внимательно смотрит в область шеи, словно выискивая подходящее место для своей пугающей цели. Вот он склонился над бывшим полным энергии телом и... Кровавый вихрь вновь засасывает все глубже и глубже, вызывая яркие картины из прошлого с безумными гонками, бесконечной стрельбой, криками сбитых пешеходов, взрывами и окружившим со всех сторон спецназом...



Александр «xtracer» Логинов (http://www.gamemag.ru)



Вы хотели эффектов? Их есть у меня!
Послесловие для маньяков Q3Radiant

ENTER

Если ты помнишь, в прошлом номере у нас был последний урок Q3Radiant. По крайней мере, я так думал. Но когда я объявил, что сага о квако-левело-строительстве подошла к концу, на меня обрушился холодный душ читательских писем, в которых ты (а это был ты, без сомнений) просил рассказать еще что-нибудь про Q3Radiant, позамороченней. Ну что ж, придется отложить мега-хитовые Warcraft 3 и Morrowind и выдать что-нибудь... позамороченней, как просили.

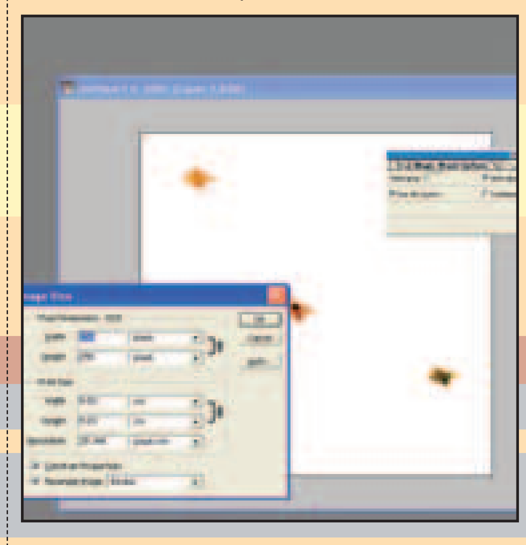
Разобравшись с элементарной архитектурой, пройдя арки, текстурирование и воду, ты готов к самой кропотливой и сложной части сражения - специальным эффектам.

Когда падает листва

Одним из самых симпатичных и облагораживающих виртуальный мир эффектов остается листопад. Пожелтевшие от осени листья кружатся в легком танце вокруг игрока, они подпрыгивают, падают и вновь взмывают вверх, создавая приятное ощущение реальности окружающего мира, а заодно отвлекая его внимание от малополигональных и неровных конструкций ;). Итак, приступим к процессу изготовления нашего зелья. Для начала возьми в руки Photoshop, PaintShop pro или любой другой графический редактор достойного производства. Используя руки и мышку, создай в своем графическом редакторе новое изображение форматом 256 на 256 пикселей. Конечно, ты можешь использовать текстуры и большего (512x512) размера, но это может вызвать нежелательные последствия для обладателей старых ускорителей.

На чистой поверхности нарисуй три небольших листа. Ты можешь не обращать внимания на детали, так как листья в данном случае лишь один из множества примеров. Ты можешь заменить их на старые газеты, дождь или снег. Внимательно посмотри на рисунок 1.

Все три листа выстроены в ряд и имеют различную окраску и степень освещения. Это важно при создании



Это не марихуана, а обычные листья дуба ;)

листопада. Ты ведь не хочешь, чтобы с деревьев падал однообразный мусор, верно? Теперь обрати внимание на правую часть меню. Видишь, мы выставили (речь идет о Photoshop) нашу волшебную палочку на ноль и включили антиальястинг? Это необходимо для того, чтобы при использовании альфа-канала листва сохранила свою свежесть, хруст и красоту. ;) Именно этим мы сейчас и займемся. Используя волшебную палочку, окрась зону вокруг листвы и создай альфа-канал (см. рис. 2).

Учти, что если твоя листва или снег имеют сглаженные углы, то создание альфа-канала может оказаться неудачным. Более того, Q3Radiant может очень серьезно глюкнуть при считывании текстур с кривым альфа-каналом.



Тот самый альфа-канал

Если ты все сделал правильно, то листва готова, и мы можем приступить к оживлению сцены. Выбрав путь наименьшего сопротивления, воспользуемся советом умудренного опытом Terry DeLaney. Для начала сохраним файл как leaf.tga в директорию

/baseq3/textures/leafs

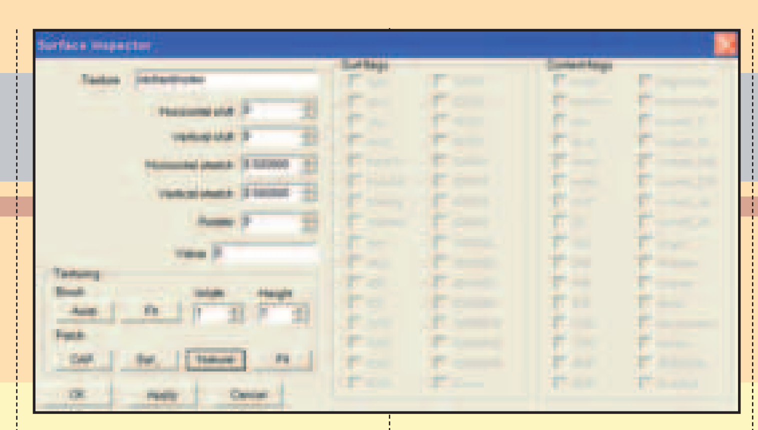
Теперь обнови shaderlist.txt (см. предыдущий номер, урок работы с Q3Radiant), добавив название нового объекта leafs, так, чтобы игра могла распознать твои листья при работе с редактором. Теперь, когда листья готовы к использованию, пришло время для написания небольшого скрипта, который оживит сцену. Основная задача состоит в том, чтобы программа анимировала наши статичные объекты в замкнутом цикле, создавая эффект реальности происходящих на экране событий. Для начала мы определим границы движения листвы. Так как листья падают строго вертикально, то мы воспользуемся командой tcmod scroll со значениями 0 и 24. В данном случае 0 означает то, что объект статичен по оси координат X, а 24 - медленную прокрутку задника по оси Y. Мы не хотим, чтобы наши листья падали нам на голову мрачными булыжниками, поэтому прибегнем к команде surfaceparm nonsolid, а для расчета поворота листа воспользуемся deformVertexes wave. Финальный скрипт (спасибо Terry DeLaney) выглядит следующим образом:

```
textures/leafs/fall_leaf_1
{
qer_editorimage
textures/leafs/leaf.tga
surfaceparm nonsolid
surfaceparm trans
cull none
deformVertexes wave 30 sin 0 10 0 .2
nopicmip

{
map textures/leafs/leaf.tga
tcMod scale 2 2
blendFunc GL_ONE GL_ZERO
alphaFunc GE128
depthWrite
rgbGen identity
tcmod scroll 0 .25

}
{
map $lightmap
rgbGen identity
blendFunc GL_DST_COLOR GL_ZERO
depthFunc equal
}
}
```

Теперь тебе необходимо создать карту с деревом, от которого будет отваливаться листва. Ты можешь попробовать нарисовать что-то сам, но я рекомендую тебе воспользоваться заготовкой все того же Terry DeLaney (http://quake3.qeradiant.com/q3afiles/tutefiles/leaves.zip).



Размножаем листву, как умеем

Когда все готово, ты можешь приступать к самому ответственному шагу - добавлению листопада в игру. Для этого возьми уже созданное или позаимствованное тобой дерево и создай вокруг него цилиндр высотой в 96 единиц и радиусом пропорционально краям кроны. Наложи на цилиндр текстуру с листвой fall_leaf_1.

Теперь, не снимая окрашивания, вызови Surface Inspector (S) и нажми (см. рис. 3) кнопку Natural.

Количество листьев увеличится, но постарайся сохранить чувство меры. Используя клавишу Fit, ты достигнешь лучшего эффекта. Теперь сохрани и откомпилируй уровень и

Тебе нередко придется сталкиваться с таким сложными объектами, как клетки, дырявые контейнеры или изрешеченные пулями двери.

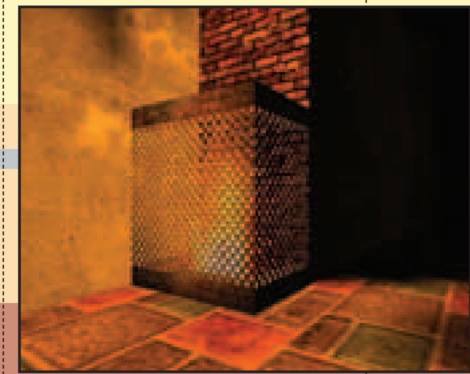
любуйся (см. рис. 4) только что созданным шедевром непосредственно в игре.

Прозрачные объекты, или виртуальное решето

При моделировании сложных уровней тебе нередко придется сталкиваться с таким сложными объектами, как клетки, дырявые контейнеры или изрешеченные пулями двери. Чтобы зря не тратить драгоценные полигоны на создание сложных конструкций, ты можешь использовать полупрозрачные текстуры. Конечно, при создании подобных поверхностей тебе придет-



И золотые листья на дубе том…



Burn, Burn, Burn!

ся повозиться с альфа-каналом (см. выше), но это уже тема для отдельного урока. Итак, приступим. Для начала тебе необходимо заставить редактор понять, что твой шадер именно прозрачный и никак иначе. Так как редактор не понимает человеческого языка, то придется прибегнуть к простому скрипту, позаимствованному из официального набора Quake 3: Arena. Скрипт для шедера base_trim/proto_fence выглядит следующим образом:

```
textures/base_trim/proto_fence
{
surfaceparm trans
cull none
nopicmip

{
map
textures/base_trim/proto_fence.tga
tcMod scale 3 3
blendFunc GL_ONE GL_ZERO
alphaFunc GE128
depthWrite
rgbGen identity
}
{
map $lightmap
rgbGen identity
blendFunc GL_DST_COLOR GL_ZERO
depthFunc equal
}
}
```

Разобравшись с элементарной архитектурой, пройдя арки, текстурирование и воду, ты готов к самой кропотливой и сложной части сражения - специальным эффектам.

Обрати внимание на base_trim/proto_fence - это путь к шедевру. Соответственно, если ты положил свою текстуру в директорию /vasypupkin и назвал ее hacker9.tag, то ты должен заменить base_trim/proto_fence на vasypupkin/hacker9.tag. Также обрати внимание на строчку tcMod scale 3 3. Эта строка определяет отношение, с которым будет отображаться в игре твоя текстура. Чем выше значение, тем ниже разрешение и хуже качество картинки. Учти, что при изменении размеров первое и второе значение должны быть пропорциональны, иначе текстура будет выглядеть испорченной. Скажем, если ты выставил ширину на 2, то и высота также должна быть равна 2. Теперь ты можешь наложить свою прозрачную текстуру на любой объект (не забудь его сделать solid), скажем, на импровизированную решетку. Сохраняй карту, компилируй и наслаждайся модным (см. рис. 5) эффектом. Если у тебя ничего не получилось - не расстраивайся - попробуй воспользоваться готовой картой Terry DeLaney (сохранять ее надо в директорию \baseq3\maps). (http://quake3.qeradiant.com/q3afiles/tutefiles/shade02.zip).

Вместо заключения

Вот и подошел к концу последний (теперь уже точно) урок по Q3Radiant; надеюсь, он помог тебе продвинуться в моделировании трехмерных объектов, а также в реализации потрясающих фантазий (почти как у Дани) и революционного геймплея. В следующий раз мы поговорим о написании модов для одной из лучших ролевых игр этого года, Morrowind. Если у тебя возникнут какие-либо вопросы - не стесняйся, пиши.

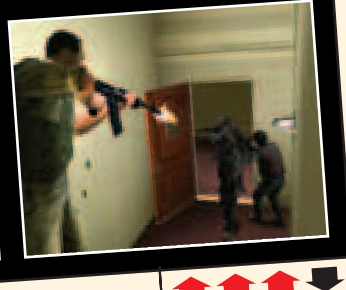
Автор выражает благодарность Eutectic и Terry DeLaney за материалы и несколько важных подсказок.



Александр `2poisonS` Сидоровский
<2poisonS@real.xakep.ru>



Урожденная	The Sum of All Fears
Жанр	тактический FPS
Похожесть	Rainbow Six
Мать/отец	Red Storm Entertainment/Руссобит-М
Требует	P2-450(P3-600), 64(128), 3D
Групповуха	LAN, Инет
Описуха	Улучшенный Rainbow Six от неутомимого Тома Клэнси. Как и в классическом R6, ты с командой довольно сообразительных напарников бегаешь/ползаешь по коридорам, кишащим террористами, и освобождаешь, взрываешь, находишь, прячешь и далее по списку. Новый движок выглядит вполне ничего, вот только жаль, нельзя свободно выбирать оружие на миссию, только один из многочисленных готовых наборов снаряжения.
ПРИГОВОР	ХОРОШО

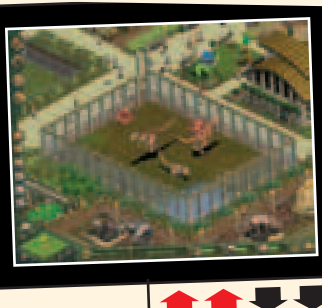
Урожденная	Hotel Giant
Жанр	экономическая стратегия (tycoon)
Похожесть	Mall Tycoon
Мать/отец	Enlight Software/Акелла
Требует	P2-450(P-600), 64(128), (3D)
Групповуха	Обломись
Описуха	Классический тайкун, на этот раз на гостиничную тематику. Получаем захудалую ночлежку, ремонтируем ее, оборудуем номера и другие помещения, нанимаем и обучаем персонал, закупаем всевозможные гостиничные примочки, и в итоге, по идее, должны получить блистательный пятизвездочный отель. Сложность ниже среднего, графика обычная для этого жанра (слегка напоминает Sims). Игра без достоинств и недостатков.
ПРИГОВОР	СРЕДНЕ




Урожденная	Mobile Forces
Жанр	многопользовательский шутер на машинках :)
Похожесть	Unreal Tournament, Redline
Мать/отец	Real Time Worlds/Rage Games
Требует	P3-500(P3-1200), 128(256), 3D
Групповуха	LAN, Инет
Описуха	Представь себе UT на колесах. Нет, покидать транспортное средство, конечно же, можно и часто даже нужно, но основной fun происходит именно в кабине джипа-ря/багги/грузовика/БМП и прочих четырехколесных агрегатов. 8 режимов игры не оригинальны, графика, местами чарующая, в некоторых случаях способна вызвать недоумение, но в целом... Не зря слова «драйв» и «рулить» относятся именно к машинам ;).
ПРИГОВОР	ХОРОШО




Урожденная	Zoo Tycoon: Dinosaur Digs
Жанр	экономическая стратегия (tycoon)
Похожесть	Zoo Tycoon
Мать/отец	Blue Fang Games/Microsoft
Требует	P233(P2-300), 64(128)
Групповуха	Обломись
Описуха	Дополнялка на тему динозавров. Теперь в твоем зоопарке поселятся птеродактили, тираннозавры, мастодонты и прочая ископаемая живность. Суть игры от этого не меняется, разве что новые строения позволяют зашибать такие деньги, что зверей можно убирать за нерентабельностью. Купи этот диск, если ты не играл в оригинал, но любишь тайкуны или если ты пробитый фанат, которому не хватало только динозавров.
ПРИГОВОР	СРЕДНЕ

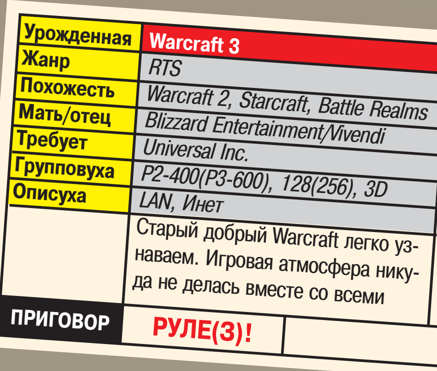



Урожденная	Neverwinter Nights
Жанр	RPG
Похожесть	Baldur's Gate 1-2, Summoner
Мать/отец	Bioware Corp./Infogrames
Требует	P3-500(P3-1000), 128(256), 3D
Групповуха	LAN, Инет
Описуха	Эпическая РПГ по третьей редакции правил D&D в знакомом по Baldur's Gate мире Forgotten Realms. Новый движок ошеломляет качеством графики и завораживающими эффектами, раскачка персонажа продумана намного грамотнее, чем в играх «старой» D&D. Игровой баланс сохраняется очень четко, монстры и AI-управляемые (на манер Fallout) NPC весьма смышленые, сюжет изобилует многочисленными ответвлениями. Must Have!
ПРИГОВОР	РУЛЕ(З)!



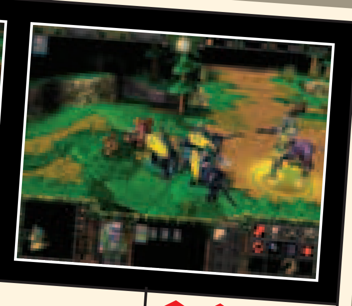



001489

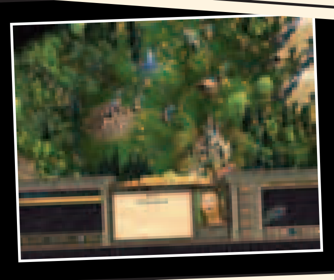


Урожденная	Warcraft 3
Жанр	RTS
Похожесть	Warcraft 2, Starcraft, Battle Realms
Мать/отец	Blizzard Entertainment/Vivendi Universal Inc.
Требует	P2-400(P3-600), 128(256), 3D
Групповуха	LAN, Инет
Описуха	Старый добрый Warcraft легко узнаваем. Игровая атмосфера никуда не делась вместе со всеми «заг-заг» и «дабу». Разве что приоделась в модное 3D. Кампания и мультиплеер представляют собой две разные игры - первая белая и пушистая с роскошным роликами и в меру оригинальным сюжетом, второй - быстрый, жесткий, беспощадный. Попробуй на себе AI в custom game - мало не покажется. Лок-тар огар!
ПРИГОВОР	РУЛЕ(З)!





Урожденная	Age of Wonders II: The Wizard's Throne
Жанр	TBS
Похожесть	AoW, HoMM 2-4
Мать/отец	Triumph Studios/Take 2 Interactive
Требует	P2-300(P3-600), 128(256), 3D
Групповуха	В ассортименте
Описуха	Походовая фэнтезийная стратегия, немного напоминающая HoMM. Как и в Heroes, отстраиваем города, набираем армию, прокачиваем героев (и не только - обычные юниты тоже качаются), исследует карту, захватываем шахты, собираем ресурсы... Графика вполне пристойна, разве что немного скучновата. Как, впрочем, и сам геймплей. Бои происходят так же, как и в Героях. Игра для тех, кому не хватило :).
ПРИГОВОР	ХОРОШО





Урожденная	Crazy Taxi
Жанр	аркадные гонки
Похожесть	Taxi Racer
Мать/отец	SEGA/Empire Interactive
Требует	P2-450(P3-800), 64(128), 3D
Групповуха	Обломись
Описуха	Порт с уже умершей приставки Dreamcast. Причем там в нее играли уже не один год. Игра была хорошей (когда-то): гоняешь без всяких ПДД по городу на такси, сбиваешь все, что плохо стоит, доставляешь пассажиров в указанную точку за ограниченное время. Сегодня старенькая приставочная игра выглядит довольно вяло и годится разве что для тех, кто уже продал свой DC, но еще скучает по его хитам.
ПРИГОВОР	СРЕДНЕ





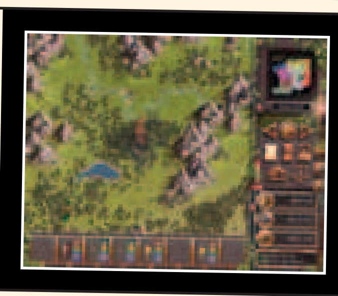
Урожденная	Zanzarah: The Hidden Portal
Жанр	адвенчура с элементами
Похожесть	Skies of Arcadia
Мать/отец	Funatics Development/THQ
Требует	P3-500(P3-800), 64(128)
Групповуха	LAN, Инет
Описуха	С элементами чего? Да всего! Тут и РПГ, и action... Игра чем-то напоминает даже Покемонов с их лозунгом «поймай их всех». Здесь «они» - это 77 фей, каждая из которых обладает уникальными возможностями, которые к тому же меняются по мере роста феи в уровне(!). Ты путешествуешь по красивой волшебной стране, решаешь загадки, собираешь и прокачиваешь своих крылатых питомцев и сражаешься с им подобными.
ПРИГОВОР	ХОРОШО





NEXT

Урожденная	Legion
Жанр	TBS
Похожесть	Caesar, EU, Takeda
Мать/отец	Slitherine Strategies/Paradox Strategy First
Требует	P233(P3-500), 64(128)
Групповуха	Обломись
Описуха	В этой стратегии ты занимаешься завоеванием земель, принадлежащих разным племенам, и их объединением под флагом Римской империи. Правда, твое участие в боевых действиях заканчивается на этапе подготовки к сражению. Ты занимаешься расстановкой войск, выбираешь формации, определяешь маневры - и все. Дальше можешь поддерживать своих лишь громкими криками. С хозяйственной деятельностью все, как обычно.
ПРИГОВОР	СРЕДНЕ





Александр `2poisonS` Сидоровский
<2poisonS@real.xakep.ru>





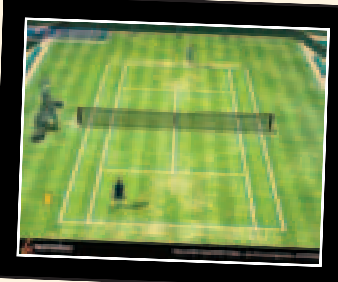
Урожденная	Syberia
Жанр	адвенчура
Похожесть	The Longest Journey, Discworld Noir
Мать/отец	Microids Canada/Microids
Требует	P2-450(P3-800), 64(128), 3D
Групповуха	Обломись
Описуха	Настоящий подарок для всех любителей поломать голову. Девушка-адвокат разыскивает некоего чувака - гениального создателя «автоматонов». Увлекательный сюжет и логичные, не раздражающие тупизной задачки тебе гарантированы. Блестящая графика, оставляющие незабываемое впечатление ролики, отличная актерская работа - в общем, все на высшем уровне. Играй и наслаждайся.
ПРИГОВОР	ХОРОШО



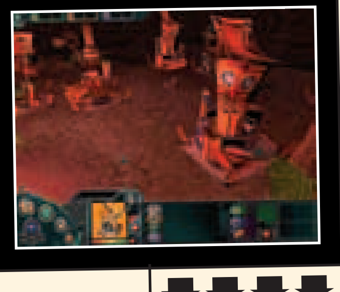

Урожденная	Hyperspace Delivery Boy
Жанр	action/puzzle
Похожесть	Bait, Dino Dave
Мать/отец	Monkeystone Games
Требует	P233(P2-300), 32(64), 3D
Групповуха	Обломись
Описуха	Удивлен увидеть здесь игру с рекомендуемым объемом RAM 64MB? А если я скажу, что эту игру сделал Джон Ромеро, отец Doom? Все дело в том, что сейчас Ромеро работает исключительно над играми для КПК, и это - порт одной из них. Простенькая аркадка про космического курьера блещет улетным юмором, прекрасными диалогами, встроенными мини-играми и абсолютно бредовым смыслом. Клевый стеб от великого классика.
ПРИГОВОР	ХОРОШО



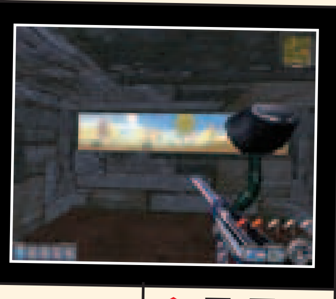

Урожденная	NGT: Next Generation Tennis
Жанр	теннис
Похожесть	Virtua Tennis, TMS
Мать/отец	Carapace/Wanadoo Edition
Требует	P2-450(P3-600), 128(256), 3D
Групповуха	LAN, Инет
Описуха	Неплохая игра для своего жанра, в девичестве Roland Garros. Реальные теннисисты, разнообразные режимы игры, включая новомодную Career, возможность открывать по ходу игры новых игроков и новые корты. Управление простое, но эффективно, вот только AI иногда подводит, хотя в других случаях оппоненты демонстрируют неплохой класс. Фишка: игра эскимосов на льду и мумий в египетской пустыне.
ПРИГОВОР	СРЕДНЕ




Урожденная	Micro Commandos
Жанр	логическая RTS
Похожесть	StarTopia
Мать/отец	Monte Cristo
Требует	P2-300(P3-600), 64(128), 3D
Групповуха	Обломись
Описуха	Отмороженная RTS-ка про крошечных инопланетян, которые, как там у них водится, собираются захватить Землю. Юнитов нужно кормить и укладывать спать, а вместо смерти они падают в обморок. Примитивная экономическая модель, напрочь отсутствующее разнообразие боевых единиц, ужасная графика и нулевая озвучка - вот что могут предложить космические агрессоры прогрессивному человечеству.
ПРИГОВОР	ЛАЖА

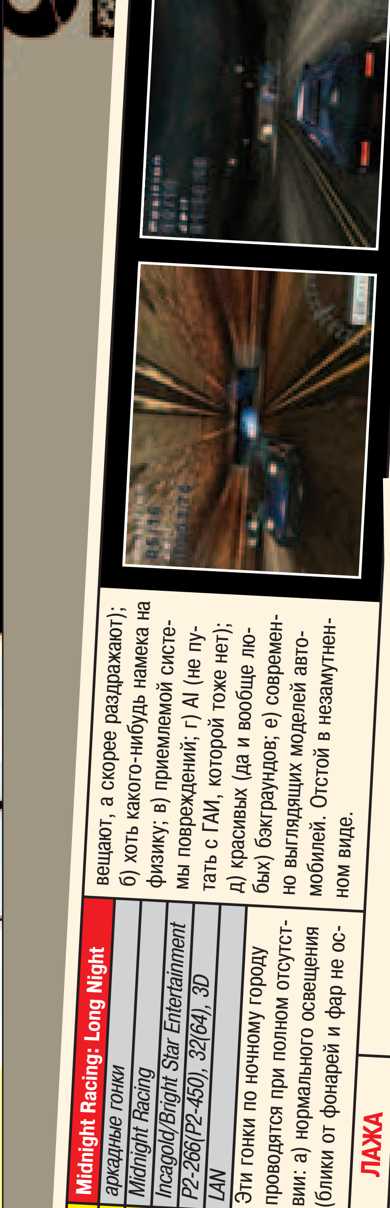
Урожденная	Extreme Paintbrawl 4
Жанр	командный FPS
Похожесть	Paintball Heroes
Мать/отец	Cat Daddy Games/Activision Value
Требует	P2-300(P3-600), 64(128), 3D
Групповуха	В ассортименте
Описуха	Симулятор пейнтбола - вещь сама по себе довольно странная. Зачем изображать процесс изображения войны, если можно просто изобразить войну? К тому же у авторов были явные проблемы с художником, дизайнером уровней, программистом AI и композитором. Игровой процесс не увлекает - поражение в плане эффекта на дальнейшую игру мало чем отличается от победы. В уровнях можно заблудиться, наскучивает быстро.
ПРИГОВОР	СЛАБО

NEXT

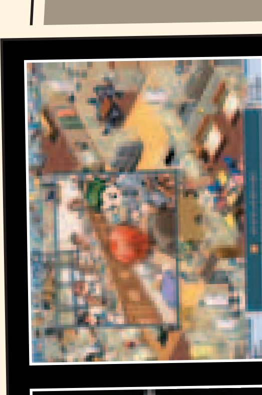

ЖУРНАЛ
МОТО
ВСЕ ОСТАЛЬНОЕ – ОТСТОЙ

Урожденная	Midnight Racing: Long Night
Жанр	*аркадные гонки*
Похожесть	*Midnight Racing*
Мать/отец	*Incagold/Bright Star Entertainment*
Требует	*P2-266(P2-450), 32(64), 3D*
Групповуха	*LAN*
Описуха	Эти гонки по ночному городу проводятся при полном отсутствии: а) нормального освещения (блики от фонарей и фар не освещают, а скорее раздражают); б) хоть какого-нибудь намека на физику; в) приемлемой системы повреждений; г) AI (не путать с ГАИ, которой тоже нет); д) красивых (да и вообще любых) бэкграундов; е) современно выглядящих моделей автомобилей. Отстой в незамутненном виде.
ПРИГОВОР	ЛАЖА



Урожденная	Big Biz Tycoon!
Жанр	*экономическая стратегия (tycoon)*
Похожесть	*The Partners*
Мать/отец	*Animedia Entertainment/Activision Value*
Требует	*P200(P2-400), 32(64)*
Групповуха	*Инет*
Описуха	На этот раз тайкуним офис. Разгораживаем огромное помещение на комнаты, покупаем столы, компьютеры, факсы-шмаксы... Нанимаем персонал, платим зарплату, устраиваем тренинги, повышаем в должностях. Короче, нормальная офисная жизнь, которую куча людей наблюдает вокруг себя ежедневно. Реализация не плохая, но и не блещет - средняя. Двумерная аниме-графика, скупая анимация, простенький геймплей.
ПРИГОВОР	СРЕДНЕ







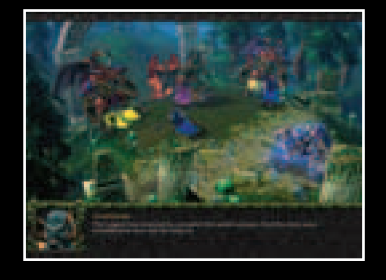


KodeMaster (cranyoblast@xakep.ru)

WARCRAFT 3

Во время игры давишь большую изогнутую пимбу на своей клаве… Нет, не эту! Зачем ты вообще положил на клаву эту большую изогнутую пимбу? Убери ее обратно и застегни ширинку. Я, вообще-то, про ENTER говорил. Нашел? Молодец. В появившемся окошке для сообщений набирай нижеприведенные коды и не забудь сопроводить их финальным нажатием на ту же самую пимбу… да не на ту, извращенец! Надпись «cheat enabled» возвестит о том, что руки у тебя растут откуда надо.

Iseedeadpeople - открыть карту (дословный перевод кода - я вижу мертвых людей);
allyourbasearebelong-tous - мгновенная победа (перевод - все твои базы принадлежат нам);
somebodysetupusthebomb - мгновенное поражение (перевод - кто-нибудь, подложите нам бомбу);



thereisnospoon - неограниченная мана (перевод - нет никакой ложки - см. кинофильм студии детских и юношеских фильмов им. Горького «Матрица»);
whosyourdaddy - неуязвимость и уничтожение врагов с одного удара (перевод - кто твой папочка?!);
strengthandhonor - продолжать играть миссию в сингловой кампании даже после того, как она провалена (перевод - сила и честь);
greedisgod - жадность это бог (перевод - дать 500 единиц золота и дерева) хм… кажется, я что-то перепутал ;).



Еще из варкрафтовских фишек: чтобы посмотреть прикольные ролики на движке, где авторы стебаются над заставками из второго WC, нужно… пройти кампанию на уровне сложности Mormal. Если хочешь посмотреть на модели юнитов из Старкрафта, опять же на варкрафтовском двигателе, проделай то же на уровне Hard.
И последнее - если начать быстро кликать на любом животном в игре, оно взорвется :).

NEVERWINTER NIGHTS

Эта игра тебе просто так не отдастся, но ведь мы на то и хакеры, чтобы добиваться всего, чего захотим, любым, даже… э-э-э… не совсем официальным путем. Для использования читов надо сначала включить режим отладки. Отлаживание программы это, как известно, процесс избавления ее от лажи, этим мы сейчас и займемся. Заходи в директорию с игрой и открывай файл nwn.ini. Там находишь строчку Game Options и прямо под ней вписываешь ключевой параметр: Debug Mode=1. Сохраняешь, закрываешь, запускаешь игру, жмякаешь тильду и набираешь в консоли почти то же самое: DebugMode1. Все, теперь она наша.



Как поднимать статсы. Это просто: вводишь соответствующий код и вместо значка # ставишь значение, которому должен равняться новый статс. Например:

SetSTR # - Накачать силу (strength).
SetDEX # - Повысить ловкость (dexterity).
SetCON # - Принять конституцию (в третьем чтении ;)) (constitution).
SetINT # - Приподнять уровень IQ (intelligence).
SetWIS # - Задрать мудрость (wisdom).
SetCHA # - Замутить стильный имидж (charisma).

Еще можно простимулировать себе уровень и количество экспы:

GiveXP # - Проинсталлировать Windows XP (с) :)) Шутка - на самом деле, набраться не по-детски. Опыта.
GetLevel # - Повыситься в уровне до желаемого размера.

Ну и бестселлеры нашей рубрики: god mode и халявное бабло - куда ж без них!

dm_god
dm_givegold #



И напоследок немного экзотики:

dm_mylittlepony - симпатичная такая мини-лошадь (пони то есть :

Остается добавить, что все читы case sensetive, то есть набирай как есть, в нужный момент не забывай до SHIFT'а дотягиваться.

GRAND THEFT AUTO III

Во время игры вводишь следующее:

gesundheit - 100% здоровья без всяких циркониевых браслетов!
giveusatank - Получаешь в подарок танк Rhino.
booooooring - Ускорение игры (не забудь вписать все пять букв «о»).
chittycittybb - …и твоя тачка взлетела!
cornerslikemad - Улучшение управляемости машины.
gunsgunsguns - Карты, деньги, два ствола… нет, три ствола… нет, ВСЕ СТВОЛЫ!
ifiwerearichman - Куча бабок - трепещите девчонки Liberty City!
ilikedressingup - Сменить внешний вид (чтобы копы не узнали, что ты в трех кварталах отсюда бросил окурок мимо урны, тссс!).
skincancerforme - «На Дерибасовской хорошая погода»
peasoup - Картина маслом:



«Ежик в тумане». Причем в роле ежика ты на своей тачке.
ilikescotland - Я люблю Шотландию! (хренакс - все небо тучами заволокло)
ilovescotland - Нет, обожаю Шотландию! (хренакс - ливень как из ведра)
bangbangbang - Большой KABOOM - больше ни одна машина не пройдет техосмотр, хе-хе :).
itsallgoingmaaad - Сумасшедшие педестрианы.
anicesetofwheels - Невидимые машины.
timesflieswhenyou - Течение игрового времени ускоряется.
madweather - Время ускоряется не по-детски.
morepoliceplease - Еще полиции, пожалуйста! - Не вопрос, сейчас доставим!
nopoliceplease - Спасибо, больше не надо! - А это уж как получится, приятель :].



nastylimbscheat - Мясо! кровище! Фрагменты тел разлетаются по окрестным районам! Неужели и сюда добралась команда по спасению рядового Райана?
nobodylikesme - Почему-то мне кажется, что меня никто не любит… Может быть, это читается в глазах пешеходов, крушащих мою машину бейсбольными битами?
weaponsforall - Манежная площадь после победы японской сборной.

UNREAL TOURNAMENT 2003

Эта игра отличается очень замороченными и сложнозапоминаемыми чит-кодами. Суди сам:

god - неубиваемость
fly - возможность полета



ghost - ходим сквозь стены
walk - ходим по земле как нормальный человек (отменяет действие fly и ghost)
loaded - все оружие и 999



патронов к нему
allammo - 999 патронов к стволам, которые у тебя уже имеются

Правда, сложные читы?

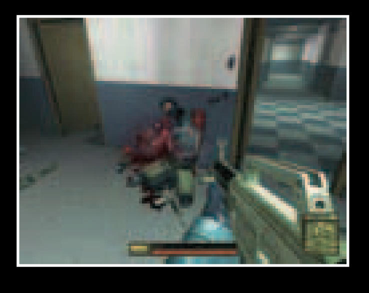
SOLDIER OF FORTUNE II: DOUBLE HELIX

В свойствах ярлыка исполняемого файла после пути (например: C:\Program Files\Raven Software\SoF2\SoF2.exe) дописываем +set console 1 sv_cheats 1. Теперь можно юзать читы. Они почти такие же как в Q3, поскольку игра сделана на этом же движке.

god - понятно что
give [название предмета без квадратных скобок] - получить указанный предмет
give all - упрощенный вариант предыдущего кода



(чтобы не заморачиваться с названиями предметов можно забрать все, вдруг что-то пригодится)
noclip - со времен Doom этим читом мы ходим сквозь стены
notarget - теперь тебя все игнорируют. Следующий!
cmdlist - список со всеми командами
map [название карты без квадратных скобок] - перейти на указанную карту
Вот список карт:
air1, air2, air3, air4, arm1, arm2, cem1, col1, col10, col2, col3, col4, col6, col7, col8, col9, finca1, finca2, finca3, finca4, hk1, hk2, hk3, hk4, hk5, hk6, hk7, hos1, hos2, hos3, hos4, kam1, kam10, kam11, kam12, kam2, kam3, kam4,



kam5, kam6, kam7, kam8, kam9, liner1, liner2, liner3, pra1, pra2, pra3, pra4, pra5, pra6, shop1, shop2, shop3, shop4, shop5, shop6, shop7, shop8, tut1



M.J.Ash (www.xknows.com, m.j.ash@real.xakep.ru)

Screen Mate Builder v 1.0

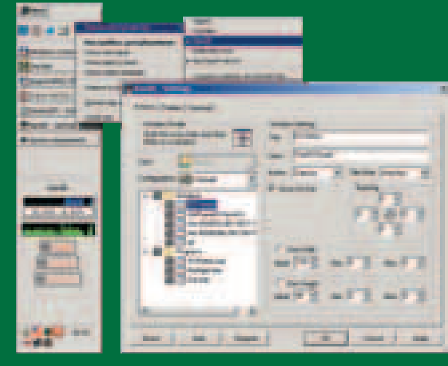
Windows 9x/Me/NT/2k/XP
Size: 927 Kb
Shareware
http://www.screenmate.net

Подборка «первоапрельских» прог, выдуманных мной для майского номера Х, получилась очень удачной. Как вспомню, сколько народа (несмотря на внушительное предупреждение о возможном розыгрыше! :) купилось, скажем, на скринмэйт Масяня - сердце радуется. Шквал писем, авторы которых требовали дать «правильную ссылку», зацепил даже Олега Куваева, который (в тщетной надежде, что от него отстанут :) поспешил написать в FAQ'е на Mult.ru о том, что подобного скринмэйта в природе НЕ СУЩЕСТВУЕТ! :) Впрочем, со столь категоричной формулировкой создатель Масяни слегка погорячился - на самом деле программа, помещающая культового персонажа на Рабочий стол, все-таки есть. Недавно я сам ее создал! Минут за десять. С помощью специального конструктора под названием Screen Mate Builder :) Правда, конструктор этот довольно простой, если не сказать - примитивный, поэтому то, что у меня получилось, мало походило на ту виртуальную Масяню, о которой я мечтал. Но бегать за курсором мыши с криком «А ты что себе вообразил, козел?» мне свое творение все же научить удалось... Хотя, если честно, то особой моей заслуги в этом нет - Screen Mate Builder может любой анимированный GIF заставить бегать за курсором и что-нибудь выкрикивать :).

Об этапах сборки скринмэйта рассказывать особо нечего: сначала тебя просят загрузить изображение в формате gif (желательно с прозрачным фоном), затем выбрать wav-файл с криком, смешным звуком или песенкой и указать, в каких случаях он должен звучать. После этого остается лишь отметить один из нескольких алгоритмов поведения виртуального персонажа на экране и получить на руки автономный exe-шник.

BandIt v 1.0

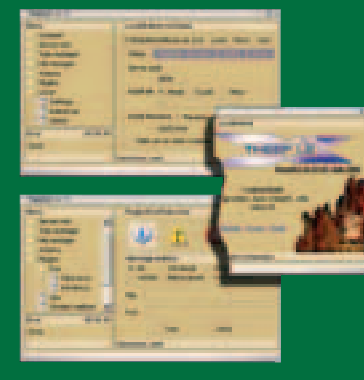
Windows 9x/Me/NT/2k/XP
Size: 725 Kb
Shareware
http://www.holesoft.com



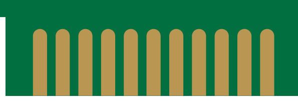
Неординарная утилита, позволяющая размещать «плавающие» окна различных приложений на панели задач. К примеру, на экране моей машины таких окон, как минимум, два - это индикатор скорости интернет-соединения программы DU Meter (www.dumeter.com) и FlashGet'овская (www.amazesoft.com) «Корзинка». Проблема с «плавающими» окнами состоит в том, что они всегда находятся на переднем плане, закрывая элементы интерфейса других приложений, из-за чего их приходится все время передвигать с место на место. BandIt помогает этого избежать. Утилита переносит и закрепляет «плавающие» туда, где они точно не будут тебе мешать. Для чего программа создает особую панель инструментов, которую после установки BandIt'a следует добавить стандартным способом (т.е. щелкнуть правой кнопкой мыши по пустому месту панели задач, переместить указатель на пункт «Панели инструментов» и отметить там требуемую панель :). Обрати внимание: запускать программу обычным способом (через меню «Пуск» :) требуется лишь при настройке BandIt'ской панели: для захвата новых окон, задания их размеров и положения. На моем компьютере «Бандит» без труда захватил все, что я ему подсунул: и DU Meter'овский индикатор, и FlashGet'овскую «Корзинку», и даже «плавающие» окна статуса ICQ. В результате у меня получилась симпатичная объединенная информационная панель, которая неплохо выглядит на экране. И это несмотря на то, что программа BandIt явно рассчитана на счастливых обладателей 17- (и более:) дюймовых мониторов, которые могут себе позволить панель задач несколько шире обычной.

TheefLE v 1.11

Windows 9x/Me/NT/2k/XP
Size: 504 Kb (server - 45 Kb)
Freeware
http://theef.4-all.org

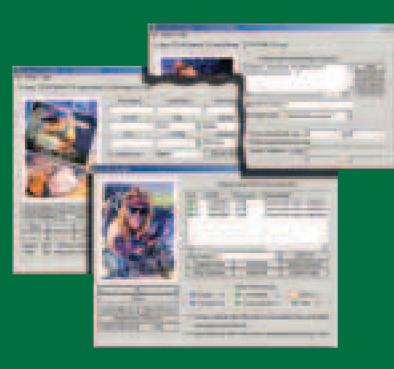


«Троянских кони» делятся в основном на две категории: тех, что мало весят, и тех, что много умеют. Первые легко попадают на чужую машину, но лишь вторые способны взять ее под свой контроль. По этой причине на удаленный компьютер чаще всего подбрасывается сперва «троянская крыса» (т.е. троян с маленькой серверной частью), которая затем и подгружает полноценную «систему удаленного администрирования». Однако существует и третья, довольно малочисленная категория троянских коней, которая делает подобное разделение обязанностей ненужным. К ней относятся трояны с наращиваемой функциональностью. TheefLE как раз из таких. Размер его серверной части - 45 кб в несжатом виде (UPX'ом сервер «утрамбовывается» до 23), что позволяет вкладывать ее в письмо или, допустим, отправлять по аське в виде картинки так же, как и любую из троянских крыс. Но после того как TheefLE обосноется на компьютере юзера Ушастого, его возможности могут быть расширены до уровня полнофункциональной системы удаленного контроля путем подключения дополнительных модулей! Каждый такой модуль оформлен в виде маленькой dll'ки. На сайте программы уже выложены модули для захвата экрана, работы с приложениями, выдирания паролей и издевательства над юзером Ушастым. Утилита для предварительной настройки сервера встроена в клиентскую часть. Кстати, даже «голый» сервер TheefLE способен передавать, получать и запускать файлы, собирать информацию о системе, закрывать «ненужные» приложения и посылать Хозяину сообщения о выходе подчиненной машины в Сеть. Немаловажным является также то, что данный троян превосходно себя чувствует под всеми версиями Окон.



Ba!amut ICQ Spider v 1.57

Windows 9x/Me/NT/2k/XP
Size: 3547 Kb
Shareware
http://www.spidercentral.com

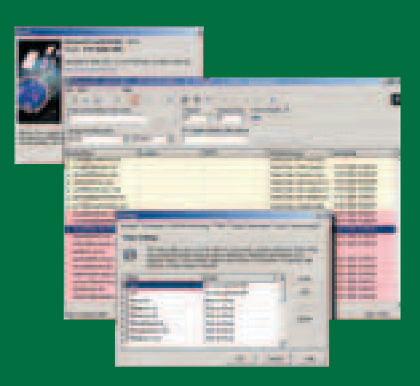


Еще один представитель нового поколения программ для массовой рассылки ICQ-сообщений. Вместо слепой «бомбежки» заданного диапазона UIN'ов (хотя это она тоже умеет :), программа выбирает юзеров, отвечающих заданным требованиям, и отсылает мессаги только им. Основное отличие Ba!amut ICQ Spider от программы IMCaster ICQ E-Marketer, рассмотренной ранее (www.imcaster.com, X № 07'02), заключается в том, что модуль поиска юзеров у нее работает совершенно независимо от модуля отправки сообщений. То есть ты можешь сначала, не спеша, сформировать базу данных ICQ-пользователей («отфильтрованных» по месту жительства, полу, возрасту, месту работы/учебы, состоянию online/offline и другим признакам), а уже затем оперативно произвести рассылку. Кстати, поскольку ICQ Spider - инструмент откровенно спамерский, то и ограничений на содержание или тип ICQ-сообщений в нем никаких нет. Более того, если захочешь, программа будет услужливо подставлять в текст каждого отправляемого послания имя, ник или фамилию получателя. По словам разработчиков, имея модем на 33,6, можно в минуту отсылать 300 - 400 сообщений или отыскивать около 700 пользователей, чьи «характеристики» соответствуют заданным. В принципе, эти цифры вполне реальные, но из-за того, что в условно-бесплатной версии есть досадное ограничение на число одновременно работающих UIN-ов, достичь указанных скоростей мне, увы, не удалось. Зато другие навороты ICQ Spider'a, такие, как защита от обрыва связи, отдельный редактор баз данных и подробный русский help (с картинками :), я и впрямь смог оценить по достоинству (хотя желания заплатить 70 баксов за полную версию проги у меня все равно так и не возникло :).

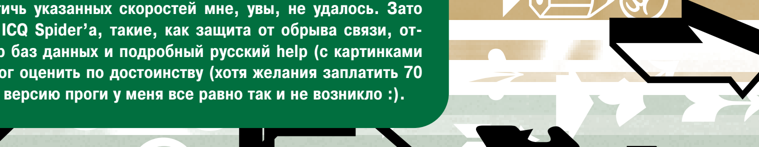
Advanced Email Verifier v 4.01

Windows 9x/Me/NT/2k/XP
Size: 1471 Kb
Shareware
http://www.glocksoft.com

На днях я закончил составлять список вида «шестизначный UIN - адрес электронной почты его владельца» (и тут же с досадой узнал, что зря две недели мучался с Assault'ом (http://icq.vsochi.com/assault, X № 07'02) - аналогичный список добрые люди уже выложили в Сети: http://yozhik.fromru.com/ICQ.zip :). Одновременно с этим мне окончательно разонравилась программа Advanced Maillist Verify (www.massmail.ru) - мой стандартный инструмент для проверки «живости» адресов электронной почты. Ее шароварная версия совершенно не подходит для проверки списков большого размера по плохому dial-up'у. Пришлось мне пересесть на конкурирующий продукт - Advanced Email Verifier (AEV) от компании G-Lock Software. Сразу же вздохнул с облегчением. Дело в том, что у AEV имеется встроенная защита от сбоев, т.е. после запуска прога продолжает свою работу с того места, на котором она была прервана. Это позволяет проверять списки за несколько подходов, не заботясь о промежуточном сохранении результатов. Помимо этого я нашел, что интерфейс AEV более информативен, а возможности настройки программы - богаче (вдобавок по Рунету давно бродит регистрационный ключик :).

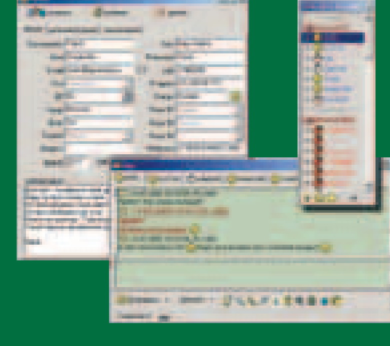


Как и Advanced Maillist Verify, AEV умеет импортировать почтовые адреса из различных источников (баз данных, адресной книгой Windows, текстовых и CSV-файлов), производить фильтрацию адресов, работать несколькими потоками и дружить с прокси-серверами… Э-э-э… Про «бесплатный» регистрационный ключик я уже говорил? :)



&RQ v 0.9

Windows 9x/Me/NT/2k/XP
Size: 841 Kb
Freeware
http://www.rejetto.com/&RQ



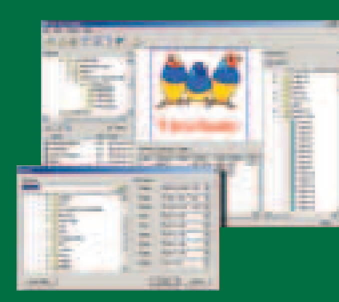
Не требующий установки клон ICQ, который можно носить с собой на дискете. Удобств - масса! Во-первых, нигде не валяются бесхозные dat-файлы, из которых любой желающий может выдрать не только пароль от твоего UIN'a, но и весь архив сообщений (Icq History Reader - http://hitu.by.ru, X № 07'02 :). Во-вторых, сама собой отпадает проблема синхронизации асек на работе и дома. В-третьих, имея в кармане дискетку с &RQ, ты получаешь свой собственный интернет-пейджер на любом компьютере (в клубе, в институте, у друзей), подключенном к Интернету. При этом за эти удобства тебе практически не приходится расплачиваться, поскольку в &RQ реализованы все по-настоящему необходимые функции ICQ, кроме, пожалуй, функции обмена файлами. Плюс имеется масса любопытных усовершенствований: однооконный механизм обмена сообщениями (мессаги от разных людей располагаются в одном окне, но на разных вкладках), возможность отсылать мессаги группам пользователей, автозамена смайликов изображениями рожиц, оригинальный интерфейс, радикально сокращающий количество кликов и путешествий по меню. При всем при этом &RQ быстро грузится, не тормозит систему (даже самую дохлую :), не показывает баннеров и не занимает лишнее место на экране.
Файлы для тотальной русификации этой проги лежат на указанном выше сайте в разделе «User-made».

ШароWARE3

M.J.Ash (www.xknows.com, m.j.ash@real.xakep.ru)

Sothink SWF Decompiler MX 2002 Pro

Windows 9x/Me/NT/2k/XP
Size: 1659 Kb
Shareware
http://www.sothink.com



Еще в раннем детстве я хорошо усвоил простую истину: чтобы понять, как что-то работает, надо это что-то взять и разобрать. Поэтому программа Sothink SWF Decompiler, позволяющая разбирать на составные части файлы Shockwave Flash, проходит у меня по разряду «обучающих». А что? Начинающие flash-кодеры и в самом деле могут применять эту прогу для обучения - она ведь раскладывает выбранный flash-ролик на отдельные кадры и декомпилирует скрипты... Хотя о чем я тут говорю! Ясно ведь, что большинство читателей Х будет использовать SWF Decompiler в качестве приспособления для выдирания звуков, текстов и картинок из любимых мультов про Масяню. А значит рассказывать надо о встроенном в программу Flash-вьювере, демонстрирующем каждый отмеченный ресурс во всей красе, и об умении программы интегрироваться в Internet Explorer, дабы вытаскивание flash-роликов из веб-страничек превращалось в легкое и приятное занятие. Что ж... Как «грабилка ресурсов» SWF Decompiler также весьма хорош: понимает flash'ки как в SWF, так и в EXE формате, строит дерево ресурсов, разрешает выбирать что, куда и в каком формате экспортировать. Заинтересовался? Тогда так, между прочим, замечу, что прогу можно скачать не только с сайта производителя, но и у F.O.S.I. (www.fosi.da.ru :)

Opera 6 Search.ini Editor 0.74 C

Windows 9x/Me/NT/2k/XP
Size: 77 Kb
Freeware
http://hitu.by.ru

Поисковый движок Оперы сделан весьма грамотно. Поле поиска с выпадающим списком поисковых систем постоянно присутствует в адресной строке. Кроме того, можно просто выделить какое-то слово или словосочетание на веб-странице и тут же отправить его одному из известных бродилке «поисковиков» в качестве запроса (правый клик мыши -> опцию Search with в контекстном меню). Само собой, стандартному ослику IE такие фишечки даже не снились. Одна беда - большая часть «поисковиков», с которыми Опера работает по умолчанию, нашему человеку на фиг не нужны. «Подружить» лучшую в мире бродилку с действительно полезными «искалками» можно путем редактирования файла searche.ini. Специальная утилита, позволяющая быстро и корректно прописать в этот файл необходимые поисковые системы, называется Opera 6 Search.ini Editor. Сделанная нашими польскими друзьями, она помогает избежать неприятной возни в notepad'е, полной творческих мук и роковых ошибок. В программе имеется солидный список поисковых систем, которые можно добавлять в searche.ini парой кликов вообще безо всякого редактирования. Правильность каждый сделанной записи можно немедленно проверить нажатием кнопочки «Тест». Интерфейс Opera 6 Search.ini Editor - многоязычный (английский по умолчанию, но русский языковой файл идет в стандартной поставке). По названию программы не трудно догадаться, что она работает только с Оперой версии 6.0 (точнее - 6.02) и выше. Opera 6 Search.ini Editor рекомендуется к приобретению всем настоящим opera'торам. Сам я с ее помощью сделал важное дело: обучил свой браузер вести поиск нужной мне инфы по конференциям сайта ixbt.com.



ХАКЕР #8(44)

»»» СОФТ

- RestoreIT! Deluxe Edition v 3.01
- Assault v 3.3
- ListMate Pro 5.42
- Advanced Instant Messengers
- Password Recovery (AIMPR) 1.33
- Icq History Reader 1.7
- Dirkey 1.3
- Extreme Picture Finder 1.4
- Flash Catcher 2.6
- Becky! Internet Mail 2.05
- Японские кроссворды 1.6
- Socrat
- Tiny Personal Firewall 3.0
- Trojan Remover 4.7.3
- Password Recovery Kit v4.0 Retail
- Pwd-Unlock 1.454 Beta
- Flame Mail Bomber
- IGMP Windows Nuker
- CPUCool 7.1.1
- RightMark Audio Analyzer 3.5
- Ad-Aware 5.82
- IngSoft Sign Of Misery 2.4
- Xteq X-Setup 6.2
- Stamina 2.3
- CuteFTP XP 5.0
- Modem Spy 2.9.2 beta
- IE 6, 5.5 SP2 patch
- MS Office XP SP1
- WinRAR 3.0 Rus

ДРАЙВЕРА

- AMD AGP Driver for Win 2000/XP
- Creative SB-Live! 5.1 Driver WHQL 5.12.1.3521
- Matrox video cards
- VIA 4-in-1 4.40 final
- Intel i845G/GL video driver 11.1
- SiS Chipset Drivers
- TEAC CD-W524E Firmware 1.0D

ЮНИКС

- Последние ядра
- XFree 4.2.0
- KDE 3.0
- RAR 3.0
- WebDownloader for X 2.02
- Web shell 1.0
- Trinux 0.80rc2
- Acrobat Reader 5.0.5
- Sylpheed 0.7.8

МУЗЫКА

- C_File new tracks
- Alien's Words
- Renoise 1.0

ДЕМКИ

- Little Nell
- My World Is How I Create It
- VIP 2
- Easter Egg
- A Fire Upon The Deep

TRASH

- Компоненты для Delphi и C++ Builder
- Исходники из "Кодинга"
- Библия Delphi-программиста
- X-курсоры
- Апд ейты к Counter-Strike
- Valve Hammer Editor 3.4
- Duke Nukem: Manhattan Project patch
- GTA3 patch
- Morrowind 1.1 patch

ХАКЕР #8(44)

TIPS&TRICKS

Способ получения халявного Инета :-). Подходишь к ларьку Роспечати (внутри бабулька копошится) и, сделав невинное лицо, просишь дать посмотреть интернет-карту. Сам незаметно стираешь монеткой pin-код и с умным видом записываешь его в блокнот. Теперь с ОГРОМНЫМИ благодарностями отдаешь карту бабульке и просишь дать тебе какую-нибудь газетку за 2 руб. (чтоб она не заметила изменений на интернет-карте). Если все получится, можешь заполнить мой е-майл тоннами благодарностей :-).

Pinkerator (pinkerator123@mail.ru) http://klub-pornushnik.narod.ru

Ведущий рубрики Tips&Tricks Иван Скляров (Sklyarov@real.xakep.ru)

TIPS&TRICKS

Как оптимально настроить файл подкачки (своп-файл) - несколько советов. Если у тебя несколько винчестеров (не разделов, а именно винчестеров), то установка файла подкачки на винт другой, нежели установлена операционная система, обычно значительно ускоряет быстродействие. Если у тебя несколько винчестеров - то файл подкачки ставится на самый быстрый из них. Если у тебя несколько разделов на винте, то файл подкачки надо ставить на самый первый из них - физически расположенный самым первым, так как доступ к этим областям винта наиболее быстрый. Целесообразно ограничить минимальный объем файла подкачки, чтобы предотвратить излишнюю его фрагментацию примерно объемом 1-1.5 объема твоей оперативной памяти (впрочем, если ты используешь графику или напрягаешь компьютер серверами баз данных, то можно поставить размером 2-3 объема RAM). Практически не имеет резона ограничивать максимальный объем, так как это может привести к сбою программ из-за нехватки памяти, а если уж и ограничивать, то никак не меньше, чем 4 объема RAM. После этих настроек комп надо перезагрузить и запустить какой-нибудь дефрагментатор (типа Norton Speed Disk), чтобы полностью дефрагментировать файл подкачки и поместить его в начало раздела. И последнее, помни, что после выключения компьютера файл подкачки может содержать твои пароли, логины, остатки конфиденциальной информации и т.п., так что достаточно "образованные дяди" из числа твоих доброжелателей или компетентных органов, загрузившись в ДОС и покопавшись в объедках твоих программ, в файле подкачки могут найти очень интересные вещи...

Garik http://www.webhowto.ru/reg

Ведущий рубрики Tips&Tricks Иван Скляров (Sklyarov@real.xakep.ru)

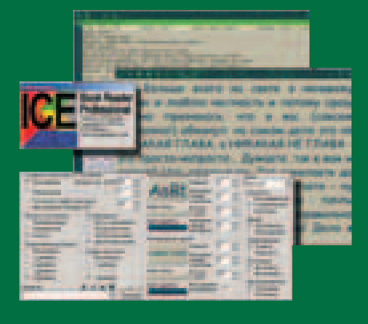
ICE Book Reader Professional v 2.4 Russian Edition

Windows 9x/Me/NT/2k/XP

Size: 984 Kb

Freeware

http://www.ice-graphics.com



Приобретение новой интересной книги я всегда считал подходящим поводом забить на все дела и провести вечер, развалившись на диване. Но в последнее время (с тех пор, как я открыл для себя электронную библиотеку Альдебаран, www.aldebaran.com.ru :) художественные произведения попадают в мои руки чаще всего в виде текстовых файлов. К сожалению, читать с экрана, сидя в кресле, - удовольствие небольшое. А плохой выбор программы-читалки может окончательно все испортить. Именно поэтому для знакомства с литературными произведениями в электронной форме настоящие книголюбы (в моем лице :) рекомендуют использовать программу ICE Book Reader. Ее главный козырь - оригинальная технология вывода текста на экран. Благодаря ей софтина может самостоятельно и с заданной степенью сглаживать неровности шрифтов (владельцы LCD-мониторов будут плакать от восторга! :), применять различные механизмы скроллинга (программный, аппаратный, DirectX), подавлять дрожание и прокручивать текст с субпиксельной точностью (т.е. очень-очень мягко :). Неплохо, да? Сразу понимаешь, насколько ICE Book Reader превосходит другие читалки, в которых, за исключением скорости скроллинга, размера, цвета и типа шрифта, и регулировать-то, в общем-то, нечего. А ведь кроме собственного «текстового движка» ICE Book Reader может похвастаться еще и целым рядом других интересных функций: автоматической синхронизацией скорости скроллинга или перелистывания с твоей скоростью чтения, правильной системой закладок, умением переформатировать любые текстовые файлы (форматов TXT, HTML, RTF и DOC размером до 1 GB) в удобный для чтения вид, а также наличием встроенных архиваторов (ZIP, RAR, ARJ, LZH, HA), позволяющих открывать текстовые файлы прямо из архива. Впрочем, хватит перечислять достоинства данной проги - пора переходить к оглашению недостатков, для которых - абсолютно фантастические системные требования. Разработчики утверждают, что для того, чтобы использовать все фишечки их читалки по максимуму, необходим процессор с частотой более 1 GHz и видеокарта типа GeForce 2 с 64 MB DDRAM на борту. Приколисты, блин! К счастью, если разумно подойти к настройке, то ICE Book Reader прилично пойдет и на значительно более слабой машине.



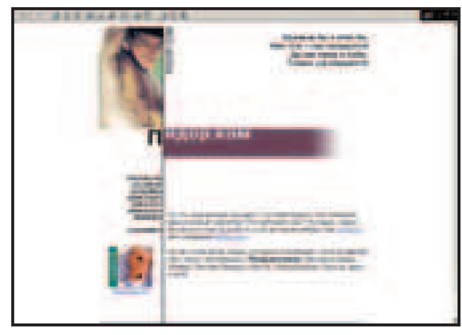


WWW

Александр '2poisonS' Сидоровский
(2poisonS@real.xakep.ru)

Pidor.com

www.pidor.com



«Ну что, красавчики, заходите - гостями будете. Как поживает ваш розовый сфинктер?» - такими словами приветствует своих посетителей pidor.com. Как подсказывает название ресурса, это не что иное, как злая и совсем не дружеская пародия на известный рунетовский гей-сайт (ссылку давать не буду, надеюсь - не пригодится). Так что если ты питаешь к российскому гей-движению теплые и нежные чувства, лучше не заходи - расстроишься. Зато если с чувством юмора у тебя все в порядке и ты не прочь постебаться над «голубой эскадрой» - это место как раз для тебя. Здесь есть все разделы, которые должны быть на любом уважающем себя гей-сайте. В рубрике «перчености» ты найдешь «реальные» истории из жизни светло-синих, на «сексодроме» тебя обучат всем тонкостям анального секса, расскажут, что такое аннилингус (тьфу, блин, аппетит на всю неделю перебили), и, вообще, проведут мощную теорподготовку. Кроме этого, ты найдешь на сайте «частушки» по теме, «пидистории», опрос «чем в кого», отзывы читателей, которых здесь ласково зовут «опидараска», и кое-что еще. В общем, будь начеку и береги тылы, амиго!

Научный иммортализм

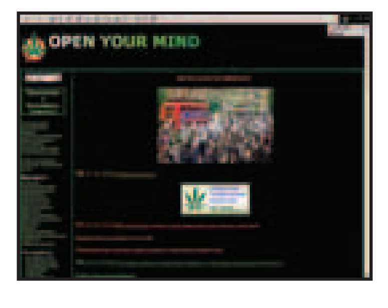
www.bessmertie.ru



Immortality - означает «бессмертие». Научный иммортализм исследует возможности и технологии для продления человеческой жизни вплоть до... бесконечности. Говорят, это возможно. С помощью наномедицины можно будет «ремонтировать» поврежденные клетки организма вживленными в человека наноботами (нет, не теми ботами, которые тебя в КС валят, а другими - совсем маленькими и выращенными специально для тебя, чтобы избежать отторжения чужеродной ткани). Кроме того, если изменить ряд генов, можно заменить обычные человеческие клетки на бессмертные. В природе существуют бессмертные бактерии и даже простейшие (например, гидра). Говорят, обнаружен неизвестный ранее вид бессмертных медуз. Пока нам остается только порадоваться за счастливые сгустки морских соплей и ждать, когда же медицина превратит нас в Дунканов МакКлаудов (или в Кощеев Бессмертных, это кому как больше нравится). Медицина обещает постараться к середине века. Твоя задача - дожить до этого светлого часа, так что уж напрягись (можешь для начала бросить курить, пить и выражаться :)).

Open Your Mind

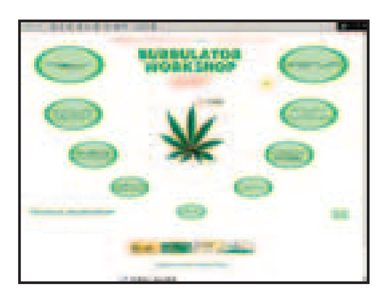
http://shinin.narod.ru



Ну а если после просмотра High.RU соответствующие выводы уже сделаны - вперед на более практический ресурс, посвященный проблемам сельскохозяйственного толка. Как и что выращивать, как освещать, поливать, удобрять, когда и как снимать урожай - все эти тонкости ты постигнешь в разделе «советы садоводам». Здесь ты узнаешь о разных сортах конопли и о том, как ее можно использовать (а конопля, надо заметить, весьма универсальное растение: хочешь - веревки вей, хочешь - одежду шей, хочешь - масло для приготовления пищи добывай, хочешь - домашней скотине скармливай, вариантов много). И если ты убедился, что без этой флоры жизнь тебе в тягость, то девятилистник тебе в руки: беги в ближайший цветочный за черноземом и удобрениями, доставай семена (они у нас в стране не запрещены) и наслаждайся своим новом хобби - домашним садоводством! А этот ресурс тебе поможет.

Burbulator Workshop Project

http://works.hop.ru



Кальян, безусловно, вещь полезная, однако не всем доступная. Да и если необходимость в кальяне возникла прямо «здесь и сейчас», то ожидание курьера из магазина может обломать весь кайф. Куда полезней практические сведения (или, как их теперь модно называть, ноу-хау) в области кустарного изготовления кальяна из подручных материалов. В народе такие устройства называются бонг (от англ. bong) или бульбулятор. Бульбуляторы обычно делают из двухлитровых пластиковых бутылок с применением таких общедоступных средств, как скотч, ствол шариковой ручки, скрепки и т.д. (возможных вариантов дизайна существует множество). На этом сайте ты найдешь практические советы по изготовлению бонга с понятными анимированными иллюстрациями, а также дизайны от читателей, среди которых встречаются и вовсе чумовые. Ну а дизайн сайта красноречиво говорит о том, какой творческий подъем может наступить у человека, грамотно изготовившего собственный бульбулятор - Арт. Лебедев отдыхает :).

Махолет

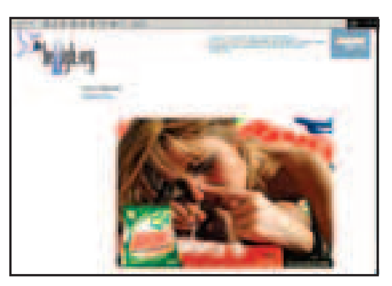
http://maholetik.narod.ru



Когда люди впервые задумались о создании летательного аппарата, они представляли себе нечто, имитирующее полет птицы, насекомого или другое летающее существо, то есть нечто, машущее крыльями. История показала, что при всем разнообразии существующих способов воздухоплавания, еще не создан ни один аппарат, который перемещался бы благодаря взмахам крыльев. Пока не создан. Однако работы над созданием таких машин ведутся, и не одним изобретателем. Оба линка ведут на сайты, посвященные созданию махолета, только в одном случае он летает как птица, в другом - как стрекоза. Преимущества махолета перед своим ближайшим «родственником», вертолетом, - высокая подъемная сила, бесшумность, безопасность, маневренность, очень высокий КПД, возможность садиться на крутой склон за счет компактных размеров и т.д. Как и вертолет, махолет будет обладать возможностью вертикального взлета и зависания в одной точке. Оба проекта получили официальный патент, оба изобретателя просят заинтересованных лиц об инвестициях для продолжения испытаний. Загляни, может, впишешь свое имя в историю авиации.

High.Ru

www.behigh.org



Подзаголовком этого сайта служит интригующая фраза «психоделическое чтиво». На самом деле, психоделическое тут не только чтиво, а вообще все - «слушево», «смотрелово», «на-линки-кликалово». Этот… хм… своеобразный ресурс посвящен измененному состоянию сознания - информационная часть сайта позволит тебе его достичь, а раздел народного творчества даст понять, что из этого получается. Лично меня просто насмерть убили публикуемые на сайте миниатюры некоего перца под ником Jaroslove, картинки «по обкурке» и «кунсткамера» - раздел с изображениями, звуками и прочей безбашенной шнягой, сотворенной явно в сильно измененном состоянии сознания.

Еще на этом сайте ты узнаешь, что из наиболее распространенных наркотических веществ конопля вызывает наименьшее привыкание (самое сильное - никотин), а также наносит наименьший вред организму (наибольший - алкоголь). Нет, не то что бы авторы сайта призывают к немедленному легалайзу, но и на мозги пропагандой не капают. Просто почитай об измененном состоянии сознания и насладись плодами его творчества.

Cryonics Institute

www.cryonics.org

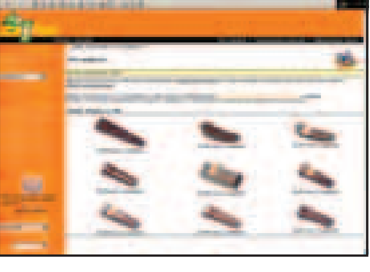


Ну, а если ты не уверен, что удастся дотянуть до полного наноомоложения, то пора действовать уже сейчас. А беспокоиться есть из-за чего: бессмертие, как я уже говорил, намечено на середину века, а это не ближайшие выходные. По данным статистики, средняя продолжительность жизни российского мужчины составляет 59 лет, так что к 2050 году ты уже будешь за финишной чертой (тебе ведь 11 уже стукнуло, верно?). На всякий случай лучше принять меры предосторожности.

Все просто: регистрируешься в Институте крионики (вступительный взнос тысяча с небольшим вечноживых президентов или по 120 баксов в год - на твой выбор) и страхуешь свою жизнь на $28000 (это еще стольник в год страховых взносов). Когда ты двинешь копыта, тебя запихнут в сухой лед и отправят в лабораторию Института. Там твою кровь заменят на специальный раствор и охладят тело до нужной температуры (-196 градусов). Так ты и пролежишь свеженьким, пока наноботы не поменяют все левые клетки на жизнеспособные и ты не вылезешь из своего холодильника наслаждаться светлым будущим. Только убедись, что ты окружен людьми, которые потратят страховые $28000 на твою заморозку, а не пропьют их на поминках :).

Cozmopipes

www.cozmopipes.ru



Давненько в рубрику World Wild Web не попадал интернет-магазин. Да, пожалуй, что никогда не попадал. А все потому, что трубки трудно найти в сети магазины, которые были бы полностью уникальны и безбашенны. Вот, первый такой попался. Cozmopipes торгует всевозможными приспособлениями для курения любых веществ, которые только умеет курить человечество. Пока ассортимент невелик, но нам обещают троекратное увеличение числа товаров уже в скором будущем. Здесь ты можешь купить кальяны, курительные трубки всех видов и форм (некоторые выглядят так, что я просто теряюсь в догадках относительно того, куда их надо засовывать и как курить), аксессуары курильщика и всяческие сувениры. Выбрав нужный девайс, достаточно добавить его в корзину, оформить заказ, как в обычном интернет-магазине, и загадочно улыбающийся курьер доставит его тебе по всей территории СНГ.



FAQ

Stepan Ilyin aka Step (faq@real.xakep.ru)

Задавая вопрос, подумай! Не стоит мне посылать вопросы, так или иначе связанные с хаком/кряком/фриком - для этого есть hack-faq (hackfaq@real.xakep.ru), не стоит также задавать откровенно ламерские вопросы, ответ на которые ты при определенном желании можешь найти и сам. Я не телепат, поэтому конкретизируй вопрос, присылай как можно больше информации.

вопрос

Мне наконец-то удалось накардить себе шелл, теперь у меня и bouncer-ы, и eggdrop-ы висят - в общем, все как у нормального человека. Только вот проблема: работать через стандартный telnet не очень-то и удобно. Подскажи, пожалуйста, какой-нибудь telnet/ssh клиент!

ответ

SecureCRT 3.4 (www.vandyke.com)

Свой мини-обзор, как обычно, начну с самого привлекательного его представителя - утилиты SecureCRT. Трехмеговый дистрибутив этой программы заставит тебя забыть о стандартном telnet клиенте или каком-либо еще терминале. Почему? Достаточно начать перечислять его функции: поддержка ssh1/shh2, возможность криптования и создания специального account-а для каждого соединения для сохранения логинов и паролей с целью их последующего автоматического ввода, огромное количество эмуляций и их настроек, поддержка firewall-а, собственный язык скриптов и многое, многое другое. В общем, программа - настоящая находка, относящаяся к разряду must have!

PuTTY 0.52 (www.chiark.greenend.org.uk/~sgtatham/putty/)

Если тебе не нужны скрипты, криптография и прочие навороты SecureCRT, то можешь смело качать небольшой по размерам дистрибутив PuTTY. Дело в том, что это, пожалуй, самый оптимальный вариант telnet/ssh клиента для обычного пользователя. Поддержка протоколов RAW/Telnet/Rlogin/SSH, возможность сохранения сессии, простой и понятный интерфейс, а также огромное количество настроек делают эту программу универсальной.

Напоследок могу предложить посмотреть и оценить IrLex (www.irlex.telemost.ru) и Secure KoalaTerm (http://www.midasoft.com).

вопрос

А что делать, если в игре нет возможности выбора импульсного набора номера, а тонального у меня нет?

ответ

Если игра написана под Windows, то, вероятно, она берет параметры набора номера из настроек модема, так что не поленись заглянуть туда. Если же там все в порядке или игра написана под DOS, то проверенем следующий трюк: вводя в игре номер телефона, по которому ты должен позвонить, поставь в начало букву «P» (это латиница). После этого, скорее всего, номер будет набираться именно импульсным набором. Фишка в том, что частенько у программ, в частности у игр, фиксированная команда набора номера - ATDT (буква t в конце обозначает, что набор должен быть тональным). Мы же, делая приставку «P» к номеру, заставляем программу передать модему следующую команду «ATDT P номер телефона», где «P», обозначающая импульсный набор, стоит после «T», поэтому модем учитывает именно ее и, соответственно, использует импульсный набор номера.

вопрос

А где в Инете можно заказать футболку с моей фоткой/слоганом/mail-ом?

ответ

Подобных сервисов сейчас просто навалом, я тебе расскажу лишь о нескольких из них, но сразу скажу, что я ничего подобного никогда в Интернете не заказывал и пока не собираюсь =).

www.ofoto.ru
Дизайн и навигация сайта сразу же производят приятные впечатления, выбор сувениров достаточно широк: доступна печать фотографий на футболке, на подставке под кружку и даже на коврике для мыши. Цены вполне приемлемые, более того - на сайте присутствуют образцы работ, так что ты всегда будешь знать, за что ты платишь. Способов оплаты несколько, начиная от банковского перевода и заканчивая оплатой наличными курьеру. Доставка по Москве курьером, по регионам - почтой.

www.linuxshop.ru
Этот online магазин известен своей любовью к linux-у, поэтому и товары здесь только *nix тематики, начиная от всевозможных linux дистрибутивов, литературы и заканчивая футболками, чашками, головными уборами с различными надписями *никсовой тематики и даже мягкими игрушками в виде пингвина. В общем, есть из чего выбрать. Цены, способы оплаты и доставки - как и в предыдущем случае. Особенно рекомендую unix-оидами, да и вообще всем любителям слова «root».

souvenir.mail.ru
Здесь продаются только красочные футболки с надписью твоего мыла на @mail.ru, которого у тебя, наверное, нет, более того, по грабительской цене в 16$, да еще и с извращенным способом оплаты с помощью сервера molotok.ru. Хотя, если ты пробитый фанат @мыла.ру...

вопрос

Здравствуйте! Я часто читаю ваши статьи, поэтому обращаюсь к вам с вопросом: как можно играть в сетевую игру по модему (не через ИНЕТ), если там модемное соединение не предусмотрено?

ответ

Отсутствие возможности модемной игры - очень странная, однако достаточно распространенная проблема. Понятия не имею, почему ведущие разработчики совершенно забыли о modem-modem игре. Но, в принципе, ничего страшного в этом нет, поскольку решить ее не составит труда. Способ, о котором я тебе расскажу, появился в далекие времена второго Quake-а. Не знаю, почему, но разработчики очень уважаемой мною компании id Software взяли и обошли возможность модемной игры стороной. Естественно, многим это не понравилось, и народные умельцы быстро нашли выход. Итак, у нас есть игра с возможностью гамиться только через специальные интернет-серверы или по LAN-у (99 процентов, что здесь используется протокол UDP, а не древний IPX). Так создадим же виртуальную сеть, построенную на dial-up соединении. Оба компьютера устанавливают в настройках tcp/ip фиксированные ip адреса, например, 192.168.0.1 (первый) и 192.168.0.2 (соответственно, второй), после чего один из компьютеров должен активизировать «Сервер удаленного доступа» (в случае win9x/me) или воспользоваться «Мастером новых подключений» в случае win2000/xp. Если в win9x/Me никаких затруднений возникнуть не должно, то случай с win2k/xp я обрисую подробнее. Зайдя в «мастер», следуй по схеме «установить прямое подключение к другому компьютеру» > «принимать входящие звонки», далее выбери активный модем и создай учетную запись (имя-пароль) для звонящего компьютера. Теперь один из компьютеров принимает звонки, соответственно - второму необходимо позвонить, используя банальный «удаленный доступ к сети». После установления соединения один из игроков создает сервер lan-игры, а второй, зная ip-шник первого, может без проблем к нему подконнектиться. Замечу, что можно поставить эти самые интернет-сервера, о которых я говорил ранее, например, для quake-ов (q2 и q3) и RTCW - это OSP Tourney, для Diablo2/Starcraft/BW - это FSGS (www.net-games.com/), для новоиспеченного Warcraft-а - это bNetD (www.bnetd.org) и все его вариации.

вопрос

Как реально заловить своего провайдера (или друга) в кидалове? Я в Интернете только почту тягаю, а счета иногда астрономические приходят! Заранее благодарен.

ответ

Что-то частенько начали приходить подобные письма. Итак, ты думаешь, что тебя кидает провайдер или друг. Случаев кидания абонентов провайдером я еще не встречал, поэтому первое, наверное, отпадает. Что же касается друзей, то это вполне вероятно, причем нагреть тебя могут не только друзья (да и друзья ли они тогда?). Как просечь? У многих провайдеров на сайте есть статистика соединений, если такая информация есть и у твоего прова, то внимательно изучи ее, и все сразу встанет на свои места. Например, у моего провайдера в статистику входят даже номера телефонов, с которых проводили соединения. Если возможности посмотреть статистику нет или ты уже, посмотрев ее, просек, что кто-то пользуется услугами провайдера за твой счет, и хочешь узнать его/ее/их номер телефона, то можно попробовать обратиться к самому прову. Как ты будешь это делать - по email-у, телефону или в офисе, дело твое, но советую именно последний вариант, это заставит работников отнестись более серьезно к твоей проблеме. Но сразу предупрежу, что они не обязаны тебе предоставлять такую информацию (если, конечно, это не оговорено в договоре), поэтому, если для тебя это так важно, то можешь воспользоваться услугами нашей доблестной милиции, обратившись с соответствующим заявлением =). Вот им-то провайдер предъявит все, что есть, и расскажет все, что надо. Если же желания общения с милицией нет, особенно если тебе есть что скрывать на своем компьютере (а они 100% будут искать на нем spy программы/трояны, проверенно на практике!), то лучше просто смени пароль и позаботься, чтобы, кроме тебя, его никто не знал.

вопрос

Посоветуй мать на чипсете KT266A/KT333 или i845d/i845e с ISA-слотом, чтобы модем можно было ISA-вый оставить!

ответ

К сожалению, это не реализуемо: дело в том, что ни один из последних чипсетов не поддерживает ISA шину, так что тебе вместе с новой матерью придется покупать и модем, тем более, тебе он, скорее всего, не помешает...

вопрос

А как можно сделать скриншот в БИОСе?

ответ

Никак. Во всех hardware изданиях «скриншоты» BIOS - не что иное, как снимок цифровой фотокамеры. Так что, возможно, теперь у тебя появился повод купить цифровик. За подробными и информативными консультациями отправляйся сюда: www.ixbt.com/digimage.shtml.

вопрос

Мне необходимо сохранять анонимность в Интернете. Подскажи, где я могу скачать списки анонимных proxy-серверов.

ответ

Искать списки анонимных серверов - дело неблагодарное и бесполезное. Почему? Да потому что 70% проксей из этих списков уже давным-давно прекратили свое существования, а большая часть из тех, которые работают, являются либо не полностью анонимными, либо тормозными, либо не поддерживающими SSL. Я же тебе советую зайти на www.proxychecker.ru или www.void.ru и, используя результаты последних проверок, найти проксю под себя. Особое внимание уделяй поддержке протокола ssl aka https (это проверяет void.ru), иначе ты рискуешь быть замеченным с настоящим ip. Да, и не советую полагаться на проверки этих серверов, всегда убедись в «правильности» прокси здесь: www.all-nettools.com/pr.htm или здесь: www.leader.ru/secure/who.html.

Ламоразмы номера:

Хочу на свою пагу натянуть чат. Как это сделать? Ответить прошу мылом. (askort31337@freemail.ru)

Как поменять пароль на Интернет? (vova13@pisem.net)

У меня проблема. Когда я переустанавливал ВиньДовс, то в режиме MS-DOS скопировал папку «Мои документы» на другой локальный диск. А когда, после переустановки, решил ее открыть, то офонарел. Она в виде обычного файла! Как мне снова превратить его в папку? (chypakyks10@hotmail.com)





НА ПИСЬМА ОТВЕЧАЛ СЕПТНЕР

ё-MAIL

Наше е-мыло: magazine@xakep.ru

НАМ ПРИХОДИТ КУЧА ПИСЕМ, НО 99% ЭТОГО СПАМА МЫ СРАЗУ ОТПРАВЛЯЕМ В /DEV/NULL

Сразу же в треш:
1. Письма с матом, пустой руганью - хамов мы не любим.
2. Просьбы выслать кряк, программу - поисковики в Инете тебе помогут.
3. Объяснить, почему не работает программа (железка) - мы не саппорт твоего софта и оборудования.
4. Вопросы в стиле «как настроить» - RTFM.
5. Просьбы прислать бесплатно журнал, компьютер, Mersedes CLK - мы сами халявщики и халяву не раздаем :).
6. Взломать/кряккнуть/фрикнуть твоего соседа, подружку, мавзолей Ленина - мы журналисты и ничего в этом не понимаем, не видели, не знаем.

А вот письма с мнениями о журнале, критикой, с идеями, предложениями, мыслями и прочим, относящимся непосредственно к журналу, - мы читаем внимательно.



Всем горячий летний привет, пропуская объемные и бестолковые вежливые предисловия обратимся сразу к главному, тем более, что и мой контрагент Исаев Дмитрий [v-drug@yandex.ru] решил похерить предисловия.

Привет Ребята. Отдельно привет, мученику который все это читает :) Обойдемся без вступления о том, что ваш журнал мне нравится, что он интересный и т.д. и т.п. это, наверное, в каждом письме написано, надоело читать:) Ну, немного покритикую и дам пару советов

1.В разделе FAQ на ответах внизу стоит печать Одобрено SINtez. Так вот, местами эта печать такая темно-синяя что текст под ней трудно разглядеть, особенно в метро, где и так не очень светло. Иногда бывает что пишите черным шрифтом на темном фоне, в том же самом метро или любом другом не очень хорошо освещенном месте читать становиться очень тяжело
2.Покритикую раздел юмора, Даня Шеповалов, у тебя в основном хорошо получается, но иногда вдохновение пропадает, если такое случается не мучайся а вставь в журнал несколько смешных анекдотов и пару забавных историй из anekdot.ru, так будет лучше всем нам.
3.Создайте раздел где будут описаны самые интересные/опасные вирусы появившиеся за 1 месяц. Место это много не займет, а получится очень интересно, да и стимул у народа появится "Мой вирус в десятке особо опасных в журнале Хакер" Будет чем гордиться 8-)
4.Теперь о ламоразмах и самых дурацких письмах номера. Мне кажется что вы 90% писем придумываете сами, всей редакцией, потому что таких людей которые вам эти письма "пишут" в природе не бывает.
Ну а теперь хочу спросить: Мне постоянно приходиться устанавливать и стирать много программ, которые после удаления оставляют свои кусочки по всем мыслимым и немыслимым местам, хард у меня не резиновый, а желания отлавливать это все в ручную нет и вот наступает момент когда видишь что установлено только самое необходимое а места все равно маловато. Слышал о программах которые отслеживают каждую вновь установленную вещь, а потом, когда ее нужно стереть, делают это до самого конца. Действительно такое чудо существует? И как мне его найти.

Теперь отвечаю по пунктам:
1. Резберемся и накажем.
2. Дане поставим на вид.
3. Продумаем.
4. А вот тут отвечу поподробнее. Никто ничего не придумывает, ибо нефиг. И так полно писем, от которых неподготовленный гражданин может потерять сознание и веру в гуманистические идеалы человечества. Поверь, в природе бывают люди и ситуации, гораздо более смешные и нелепые, чем вообще можно себе представить. Так-то.
5. Программы такие есть и их много. Выбор зависит от конкретной операционки, лично я пользовал Second Chance под 9x. А по поводу остальных возможностей тебе помогут наши многочисленные читатели. Помогут ведь?



Alibek Hackerov [hackerov@mail.ru] отправляет нам (по его же словам) уж четвертое письмо. Похвальное упорство, которое решено немедленно вознаградить немедленным же опубликованием.

Приветствую свой любимый журнал. Причем любимый не зря. Это, кажись, уже четвертое мое письмо к вам, но и оно не претендует на публикацию. Должен сказать, изменения в журнале вижу только позитивные. Однако есть рудименты, от которых надо избавляться: статьи про игры и про кибер-спорт - в особенности. Кому надо, тот должен много тренироваться, он уж сам будет всегда в курсе, где и когда какой чемп проходит. А ваши статьи заставляют ламаков развешивать уши и читать про то, как крутой мужик Полос всех делает (я сам ламер, но в игры не играю - просто не нравится мне). Хотелось бы видеть взамен всяких Джойстиков больше статей про сетевые протоколы и все такое, линух (хочу взять его за клюв). В "Кодинге" просьба предпочтение отдавать сетевым штучкам, графикой не увлекаться, потому как для такого обывателя, как я, статьи про нее ничего не оставляют, кроме как тупо копировать ваш код. А если кому надо будет - для этого книги есть. И еще... В "Кодинге" или где-то еще хотелось бы лицезреть артиклы про веб-программинг (пхп и перл). Что касается вашего CD... Именно то, чего я так долго хотел, вы нам и выдали. Только просьба катать туда проги не только из Шаровар, но и все те, что упоминаются в остальных статьях журнала. Только разделы "Демки" и "Музыка" я не заценил. Вкусы разные... А диск не резиновый, поэтому всех меломанов вы по-любому не удовлетворите, так уж пусть вместо музыки будет софт. Отдельный привет Дане Шапковалову... Помнится, в предыдущих письмах я и его просил убрать... туда же, куда и Джойстик. К своему ужасу должен сказать, что его статьи уже не вызывают у меня такого отвращения, как прежде. Три полосы этому [cut] можно выделять. Я вовсе не хочу сказать, что ваш журнал должен быть сурьезным, как книга по Си++, поэтому и X-life, и ЗападлУСтроению суждено на его страницах быть.



А вот и несколько другое мнение, которым с нами не замедлил поделиться Антон Нечаев [bl1tz@rambler.ru]

Дарова,100-килограммовый!(для средних умов-100кг=центнер-))... Передупреждаю сразу, что буду катить бочки на г-на urinix'a! (первое-же письмо в X №06.02{urinix@infonet.nnov.ru}) Ты пошто на{censored} "толстого"(сорри) обидяешь! Понимаешь, если про новинки МАЙТЕКА не писать, то будет шо-то страшное... (наблюдал молодых людей, которые тыкали пальцем в ЯБЛОЧНЫЙ MAC, у меня спрашивая:"Это LINUX?..:-}") И игры низя забывать! Ты же не хочешь просидеть у моника всю жизнь, наблюдая исходники:-(Надо развиваться и познавать, что такое SUPERMARIO... А данюю ваащще не трожь...он is the power!!! Ты еще говорил, что больше о технологии хака писать надо. Шо эта за ксакеп такой, коли сам не мотыжет:-) Слышишь, X? Все пучком на{cenoired}! pony'sprite'C@$!O З.Ы.чаво ваш диск не с першага разу попер читаща?-(



2-ой приз

Третим в этой "связке" хотелось бы поместить послание от Cosinus-а [cosinus@pisem.net], который не парится по всяким там мелочам и мыслит масштабно, высказывая свое мнение, например о ситуации в компьютерном мире в целом. Так держать!

Привет, ребята из Хакера!!! Вот читаю я письма из е-Майла и думаю, что пришло и мне высказать свое мнение о Вашем журнале и вообще о ситуации в комп-мире. Я читаю Ваш журнал с начала этого года. По письмам читателей, полагаю, что дизайн журнала существенно изменился. Я не видел журнала до этого, но нынешний дизайн мне очень нравится. Благодаря Хакеру я стал больше понимать в компьютерах. И пусть я пока зеленый ламер, но это не надолго - все может круто измениться. Я собираюсь поступать в этом году в университет и выбрал специальность "Автоматизированные системы управления" (зацените выбор).

Так, следующая часть письма будет наездо-ругательной >:(На страницах журнала и в письмах читателей очень часты наскоки на Микрософт и ее детищ. Так вот лично я считаю, что Окна (начиная с 98SE) - это грандиозная работа, выполненная прогерами Билла и не стоит винить их за то, чо иногда они работают не так, как надо. Последнее творение конюшни Микрософтовских - XP - это вообще что-то необыкновенное. С Линуксом я познакомился совсем недавно - они произвели на меня такое же впечатление, как новая игрушка для ребенка. Ну посмотрел как выглядит, как работает, но не знаю, что с ней делать :(В общем, спасибо Вам, развивайтесь (не забывая нас - Ваших читателей) и всяческих Вам успехов. С уважением, Cosinus.

P.S. Насчет писка в системнике Славяна (]['ver 06.02(42)). Это пищит вирус, который располагается в конденсаторе на пятой строчке во втором столбце таблицы размещения файлов на первом разделе пятой главы книги "Гарри Поттер и Вирус-самоубийца".

Что касается второй части письма: это всего лишь мое скромное мнение, но тем не менее… Итак, сдается мне, что для каждой работы должен быть свой инструмент. Забивать гвоздик отверткой не совсем удобно, как и затачивать карандашик лобзиком. Вообще говоря, мне иногда как-то дико слышать. что "линух круче виндов" или наоборот. Какой в этом смысл? По каким критерия лучше? Для кого? Ведь не приходит же никому в голову сравнивать жигуленок и последний бимер в ситуациях, когда надо привезти с дачи мешок картошки или образцово-показательно отправиться в ночной клуб. Разные цели - разные решения. Так что пользуйся тем, что удобно именно тебе и поменьше внимания обращай на подобные, мягко скажем, не совсем корректные сравнения.



DEFENDER представляет самое дуратское письмо номера

То, что ты прочтешь ниже - не бред. Наоборот, послание содержит скрытый глубинный смысл, смысл которого смогут постить лишь избранные. Шикарное изложение, Маркс с Энгельсом и Троцкий с Каутским отдыхают, нервно куря за дверью…

Re[v]erS [hidden@rol.ru]

Прива!!! Ворнинг - нижеследующие строки можно (а иногда и нужно) считать кодированным письмом. Знающие люди меня поймут. При себе иметь: инфракрасные очки, свечку, 2 и более шифровальщика (ну или как их там - криптолога, что ли ?)… Итак, начнем: Привет, дорогая бабушка !!! Пишу тебе из далека ;] !!! Вот хочу купить (!!!)…эээээ….коробку конфет с начинкой, но нигде не найду. У нас вообще трудно…..их найти. Благодарен тебе за то, что ты пишешь такие замечательные…ээээ….письма !!! Они мне оЧЧень помогли ;] … Кстати, собака залает в конце недели, так что не помешало б убрать посев !!! Что еще??? А вот, великолепно ты придумала с этим каналом по телевизору. Как он называется?? Ах да, Кодинг. Мой самый любимый. А че тама Мурка-то ??? Жива??? Ну, и хорошо. Сегодня увидел на заборе знак "][". Ты не знаешь, что это значит??? Я у всех друзей спросил - не знают. Интересно, что это такое? В общем, желаю тебе, чтоб весь твой урожай взошел и вырос. Продолжай в таком же духе. И последнее - лошадь сдохла…=) С уважением, Re[v]erS.

К письму Alexey-я [Alexey1@mail.samtel.ru] особенно-то комментарии и не нужны, но…

Здравствуй дорогая редакция! Пишет Вам ваш постоянный читатель. Я читал много журналов, которые так или иначе затрагивают тему компьютеров, но все они читаются в охотку. Ваш же журнал отличается тем, что всегда читается с большим интересом. Не могу сказать, что всегда читаю журнал от корки до корки, но, не смотря на это, он меня многому научил. Долгое время Ваш журнал был практически единственным источником информации для меня. Из него я узнавал новости о "железе", о новых программах, кучу полезных советов. Особенно интересны для меня статьи про настройку оборудования, программ, описание различного нового софта. Совсем недавно я обзавелся INet'ом и, у меня появилась возможность общаться с вами. Первым делом послал письмо в FAQ с наболевшим вопросом. Честно говоря я не ожидал такой оперативности, ответ пришел на следующий день. Огромное спасибо Stepan'у за ответ. Теперь собственно о том, о чем я и хотел сказать. В своем ответе на одно из писем Вы сказали, что тираж Вашего журнала именно такой, какой на него спрос. Я, конечно, не могу претендовать на объективность суждения, но мне кажется, что все же небольшой дефицит в виде нехватки ваших журналов все-таки есть. По крайней мере, в нашем областном центре достать его без проблем практически невозможно, раскупают в первые два дня после его появления в киосках. Ну а в нашем городе его вообще в продаже нет. Хочется еще попросить, чтобы Вы все-таки делали небольшую скидку на начинающих пользователей, которые еще плохо разбираются в терминах вашего сленга. Ну и напоследок хочется пожелать Вам больше читателей, а нам больше интересных статей. Привет всей редакции.

…но возвращаясь к теме дефицита и доступности журнала напомню еще раз, что Х - это всего лишь товар с точки зрения рынка. Есть продавцы, которые занимаются доставкой журнала по городам и весям, есть покупатели, которые там живут-поживают. Да, понимаю, не особенно приятно, когда именно тебе не достается лишний экземпляр. Значит надо бороться с такой ситуацией. Как я бы поступил на твоем месте? Я бы договорился с конкретным продавцом о том, что один экземпляр он будет откладывать для тебя железно. Можно даже небольшую предоплату ежемесячно делать. Продавец спокоен, а ты доволен. Есть мнение, что в подобной ситуации это одно из самых разумных решений…

Хумор

Даниил Шеповалов (dan@real.xakep.ru, www.danya.ru)

Он сказал: «Поехали!», или жизнь по дзэн

ГЛАС НАРОДА
(Результаты соц. опроса на тему «Кому бы я оторвал яйца?»)

PUNK И TROJAN: Мы хотим оторвать яйца Егору Петрову (нашему хорошему товарищу).
ЛЕНА: Я хотела бы оторвать яйца Толкину!
САНЕК: Нашему преподу по экономике Богатыреву Владимиру Ильичу.
НЕИЗВЕСТНЫЙ: Я бы оторвал яйца Андрею Малахову и вырвал матку Юлечке Меньшовой.
DERRER: Папе, 18 лет назад.
ЮЛЯ: Я очень хотела бы оторвать яйца своему псу за изгаженный вновь ковер.
МОНАХИНЯ: Пи-асу, который злостно хочет поиметь мои винды во все дыры.
ДМИТРИЙ: Я бы оторвал яйца своей любимой девушке и двум гопникам-одноклассникам, из-за которых я не иду на выпускной!
РОСТИСЛАВ: Оторвал бы их той с-ке, что украла мой сотовик.
RASTAFARI: Всем членам Госдумы за их гнилые базары ни о чем...

Ну а победителем нашего конкурса единодушно признан jicc (jicc@mail.ru) за следующий опус: "Неправда, что старушкам оторвать нечего! Можно пришить, подождать, пока подзаживет, а потом оторвать, а потом опять пришить и т.д.
З.Ы. А что, Б. Гейтсу уже оторвали? По DirectX 8 SDK этого не видно."

Даня: миф или реальность?

Вот уже несколько долгих лет прогрессивную общественность терзает один и тот же вопрос: "Что (или кто) такое Даня Шеповалов?". И какого хрена четыре года подряд в каждом номере научно-популярного журнала "Хакер" публикуется параноидальный бред, подписанный этим именем? Сколько читателей][- столько и мнений по этому поводу. Приведем лишь некоторые из них:

■ 1. Даня - это альтер-эго Сергея Покровского, который страдает перманентным расщеплением личности.

■ 2. Даня - это генератор псевдослучайных предложений, написанный Доктором Добрянским на языке "Алгол-68".

■ 3. Даня - это говорящий попугай-гермафродит Родригес, которого Покровский раз в месяц кормит галлюциногенными грибами, вымоченными в PCP.

А теперь самое время для сенсационного заявления: дело в том, что мы не знаем, кто такой Даня Шеповалов. Его тексты мы каждый месяц находим под дверью редакции в полнолуние. Более того, у нас есть подозрение, что и сам Даня не знает, кто он такой...

Он живой и светится!

■ Вспоминает Антонина Ивановна Крайзеншпиц, классная руководительница:
Ой, вы знаете, такой был милый мальчик поначалу. А в четвертом классе вдруг написал сочинение "Цифровая сперма". Мы думали, ему Нобелевскую премию по литературе за него дадут. А потом Даня музыкальную группу организовал с этим же названием. Первый альбом (на бобине) у них через месяц вышел. Назывался "Детский Церебральный Паралич". Мне там третья песня очень понравилась... там еще такой припев был... забыла... а-а-а... "Лиловый говнопанк в душе моей расцвел"!

■ Олег Рамзесович Бздрищенко, глава школьного кино-кружка:
Мы тогда американскими фильмами увлекались, вот и решили сделать продолжение "Звездных войн". Ну, разумеется, сценарий нужен был - Даню попросили придумать, он тогда хорошие сочинения писал. "Цифровую сперму" его читали? Зря! Настоятельно рекомендую, там один момент хороший есть, где маленького ослика... неважно, в общем. Ну, короче, написал он нам сценарий. Там, значится, весь фильм Звезда Смерти уничтожала мощным лазерным лучом обитаемые планеты. Одну за одной. По две планеты в минуту. Итого за одну серию 180 космических взрывов было. А Даня не поленился - написал сценарий десяти серий.



Даня в детстве

■ Настя Мазина, продавщица универмага "Серебристый":
Не может быть! Так это, значит, сам Даня был! А я-то, дура, все думала, что это за чудила такой. Он к нам в магазин целый год приходил каждую ночь ровно в 2:15, кидал в корзинку бутылку водки и тюбик вазелина, а затем проходил через мою кассу. Знаете, улыбается весь такой, смеется...

■ Аркадий Помахайло, капитан милиции:
Ага, помню, конечно, да его к нам в отделение чуть ли не каждый день доставляли. Ну, под Новый год он завсегда у нас отдыхал. А в чем дело-то все было: ему, видите ли, не нравились все эти поздравительные растяжки с надписями "С Новым годом, дорогие петербуржцы!". Дескать, скучно это и убого. Вот Даня и вешал самостоятельно в ночь на 1 января на Невском белоснежную растяжку, на которой метровыми черными буквами было написано "Х.Й". Да много чего было. Вот хотя бы случай на рынке.



Рубрика «Я плакал» (самое-самое письмо Дане)

from: Чикин Олег
(baza@monch.mels.ru)

Ничего тебе писать не будем, потому что приведенная ниже фотография как нельзя лучше передает наше отношение к твоему творчеству.

Он тогда оделся моджахедом и продавал с лотка противотанковые гранаты. А за спиной у него большой зеленый флаг стоял с надписью "Все для фронта! Все для победы!".

■ Ольга Кондратьевна Зюй-Заколдырская, директор школы:
Очень талантливый мальчик: сочинения хорошие писал, песенки, в жизни школы участвовал, не пил, не курил. Правда, вот на последнем звонке Даня меня немного расстроил. Представьте себе только: праздничная линейка, учителя, родители, выпускники читают стихи, посвященные школе. И тут вдруг на середину актового зала выбегает учитель физкультуры в девичьем матросском костюмчике, с бантиком на голове и колокольчиком в руке, а из-под коротенькой юбочки у него выглядывает, простите за выражение, здоровенный волосатый член до колен. И вот, значит, наш физрук около получаса бегает по актовому залу, размахивая своим достоинством, позванивая колокольчиком и выкрикивая что-то о боевых слонах, которые напали на девственниц города Рамакитешвар. Так вот, оказывается Даня накормил его в тренерской какими-то таблетками от радиации и дал почитать "Бхагавад Гиту"...

■ Лора, девушка Дани:
Я с ним однажды целый месяц жила. Такого насмотрелась, не приведи Господь! Например, каждую ночь, ровно в 2:30 он выкрикивал изо всех сил (чтобы соседи слышали) одну и ту же фразу: "Не жалей бензина! Сожжем их всех!!!" - и включал на максимум главную музыкальную тему из фильма о Шерлоке Холмсе. Хм, еще у него дома повсюду книги валялись. Я даже помню названия некоторых:
- J. Thompson "Suicide Freestyle"
- К. Айзенковский "Что делать, если за вами следят из космоса"
- А. Ахмедбеков "Глянцевые журналы как орудие джихада"
- Р. Максимов "Напалм для чайников"
- С. Джамунишвили "Реактивные психозы при алкогольных ремиссиях"
- К. Чуковский "Мойдодыр, Тараканище и другие бытовые галлюцинации"
- Д. Мааресков "Роботы - высшая ступень эволюции"
А на меня он внимания вообще не обращал. Мы и не целовались-то даже ни разу. Только в зоопарк часто вместе ходили - он это дело очень любил, особенно у вольера с осликами всегда много времени проводил. А ушла я от Дани, когда он начал носить черные сапоги на высоком каблуке и называть себя Констанцией.

■ Алексей Разумихин, известный издатель:
Ну да, как-то Даня приходил ко мне. Принес написанный им дамский роман, типа Даниэлы Стил что-то. Только мы его не напечатали. Почему? Да потому что он заканчивался приблизительно так: "Заходящее солнце скользнуло своими томными, ласковыми лучами по нежной коже девушки, а легкий летний бриз растрепал ее длинные волнистые волосы. Это зрелище окончательно свело с ума Леонардо: он положил руку на упругое бедро Алисы и страстно припал к ее устам. А потом трахнул! Два раза!".

■ Антон Пластилинов, знакомый:
Ага, мы с ним вместе одно время донорами спермы подрабатывали. Неплохой парень, только шутки у него дурацкие. Проходим мы, допустим, медицинский контроль перед сдачей материала, уже почти конец, а он вдруг хлопает меня рукой по плечу и кричит: "Эх, офигенно мы вчера в бордель съездили! А кокаин-то какой классный был!!!".



Даня употребляет

X-MUSIC

Музыка для хакера

Команда: Целая обойма матерых и не очень музыкантов
Пластинка: Детский сад штаны на лямках
Релиз: Real Records, 2002
Реальный хит: Мария, Мирабела

Ну и сборничек... В меру детский, в меру взрослый, а главное - забавный и веселенький. Все композиции сгруппированы в 3 сета, каждому из которых присвоено собственное суб-название:»Вонзим?», «Погрустим?» и «Оттянемся?». Музыкальные монстры-исполнители, в числе которых Чичерина, «Мультfильмы», «Кукрыниксы», «Леприконсы», «Ногу свело», «Тайм-Аут», «2 самолета», Найк Борзов и прочие-прочие оттягиваются по полной программе, задушевно выводя рулады на темы до боли знакомых и родных фильмов и мультфильмов. Супер-сборничек, всем слушать по пять-семь раз, ожидая наступления счастья!

Музыка для крякера

Команда: DJ Antonie
Пластинка: Houseworks, volume 3
Релиз: Gema, 2002
Реальный хит: Orange - Can you feel it

Некоторые называют подобные музыкальные шедевры диско-хаусом, некоторые их никак не называют, а просто слушают. Да ведь есть чего послушать-то если быть честным. Забавные, выразительные треки, которые для всех желающих мощно замиксовал широко известный в узких кругах DJ Antonie. Сейчас подобная музыка довольно популярна в демократичных клубах, так что не отрывайся от коллектива, слушай, танцуй, получай заслуженное удовольствие.

Музыка для западлостроителя

Команда: Yann Tiersen
Пластинка: Саундтрек к фильму Amelie from Montmartre
Релиз: Victoires Productions, 2001
Реальный хит: Да любой!

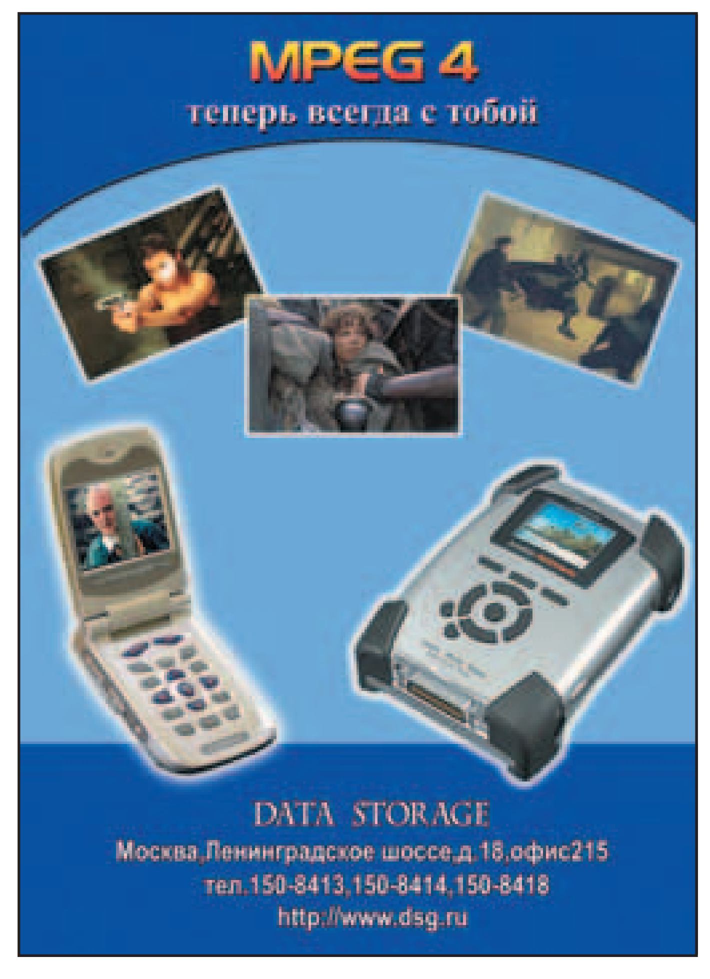
Ян Тирсен, молодой «кельт», талантливый француз, композитор, дирижер, музыкант и чистой воды романтик. Ничего удивительного в том, что его музыка стала неотделима от фильма Amelie from Montmartre нет. Если вообще можно совместить два очень добрых мира в один - то это уже произошло, просто посмотри сам фильм и попробуй представить его без музыки Тирсена. Очень «французская» музыка рождает сама по себе отличное, расслабленное настороение, не позволяя даже и подумать о каком-то там западлостроении. Так что вперед - за альбомом и попробуй почувствовать разницу. Не обломаешься.

Музыка для warezника

Команда: Сборник
Пластинка: Clubers guide to Ibiza 2002
Релиз: Ministry of sound recordings, 2002
Реальный хит: PPK - Reload

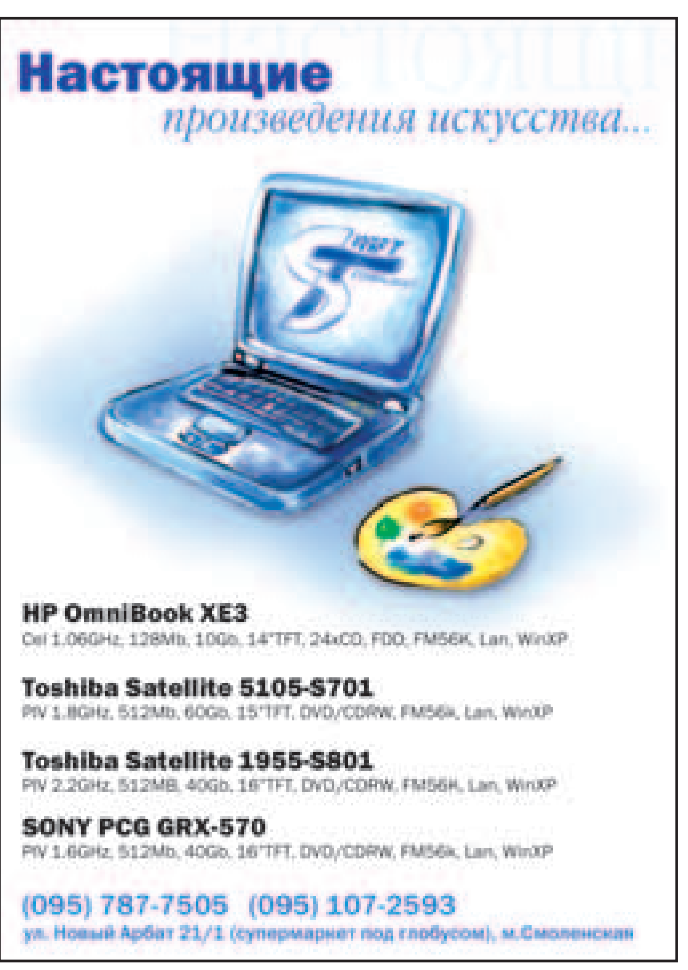
На дворе лето. Всякие там отпуска, новые встречи, знакомства, тусовки, мальчики, девочки, коктейли, романтические закаты и рассветы. Но не стоит при этом забывать, что внутри каждого из нас сидит эдакий «энерджайзер», так и стремящийся вырваться наружу и забиться в экстазе танца. В тот самый момент, когда ты утратишь контроль над своим внутренним «энерджайзером» - воткни ему один из двух компактных дисков сборника и попробуй проследить за реакцией. Есть мнение, что мало не покажется :)). Выбор настоящего отвязанного летнего клаббера, рвущегося в волны моря и музыки.

Приём объявлений в раздел Classified e-mail: avdeev@gameland.ru Тел.: 229-2832 229-4367


MPEG 4
теперь всегда с тобой
DATA STORAGE
Москва,Ленинградское шоссе,д.18,офис215
тел.150-8413,150-8414,150-8418
http://www.dsg.ru


ROVER BOOK
ВСЕГДА
В КУРСЕ ДЕЛ
НОУТБУКИ
ОТ КОМПАНИИ
ИНДЭЛ
1295
1375
Indel
ИНДЭЛ
Москва, м. Профсоюзная,
Нахимовский проспект, 36
129-21-36
124-85-13
124-87-09
ГДЕ БЫ ТЫ
НЕ НАХОДИЛСЯ...


Алетон
№ РОСС RU.AR-46 B57607
товар сертифицирован
КОМПЬЮТЕРЫ
ДЛЯ ДОМА И ОФИСА
Продажа компьютерной техники в КРЕДИТ
Сборка, модернизация компьютеров
Проектирование, монтаж, обслуживание локальных сетей
Подключение к Интернету
комплектующие, мниторы, принтеры,
сканеры, fax-модемы, оргтехника,
картриджи, аксессуары
компьютеры для офиса
ATX/ASUS/Celeron900/128Mb/HDD10Gb/SVGA8Mb/FDD/CD52X/SB - 300
компьютеры для дома и офиса
ATX/Epox8KHA+/AMD XP1700+/256DDR/HDD 40GbIBM/GFMX400 64Mb/FDD/CD52X/SB - 515
домашний компьютер ATX/ASUS P4t-E/P4
1700/256 RIMM/HDD 40GbIBM/GFMX400 64Mb/FDD/CD52X/SB - 670
полная гарантия 3 года
www.aleton.com
м. "ТРЕТЬЯКОВСКАЯ" ПЫЖЕВСКИЙ
пер., д.5 офис 121 (1-ый этаж), с 10 до 20
956-4996
737-6204
м. "МАРКСИТСКАЯ"
ул.МАРКСИТСКАЯ, Д.20, корп.6
911-9134


Настоящие
произведения искусства...
HP OmniBook XE3
Cel 1.06GHz, 128Mb, 10Gb, 14"TFT, 24xCD, FDD, FM56K, Lan, WinXP
Toshiba Satellite 5105-S701
PIV 1.8GHz, 512Mb, 60Gb, 15"TFT, DVD/CDRW, FM56k, Lan, WinXP
Toshiba Satellite 1955-S801
PIV 2.2GHz, 512MB, 40Gb, 16"TFT, DVD/CDRW, FM56K, Lan, WinXP
SONY PCG GRX-570
PIV 1.6GHz, 512Mb, 40Gb, 16"TFT, DVD/CDRW, FM56k, Lan, WinXP
(095) 787-7505 (095) 107-2593
ул. Новый Арбат 21/1 (супермаркет под глобусом), м.Смоленская

Юниты

Борда

Мессадж можно закинуть на
board@real.xakep.ru

WARNING!!!



Объявления рекламного характера не публикуются!

1. мы не будем рекламировать твою страничку, сервер и прочее
2. все письма с матом и прочей шнягой удаляются сразу
3. мы постараемся размещать сообщения в ближайших номерах, но ничего не обещаем :)

OK





Питерцы! Просьба к счастливым обладателям компакта ИЮЛЬСКОГО номера(за 2002, конечно), не мог бы кто копирнуть CD! Об оплате договиримся - не проблема. **SpillOver@xakep.ru**

Ищу друзей по переписке. Откуда бы вы ни были, пишите! С москвичами могу встретиться в Rl и вместе попить пивка :)). В общем, мыльте на **fi0nar@freemail.ru**. Жду!

Создается западло-группа. Нужны люди в Москве. Набор до Октября. Мыльте на **dpbers@rambler.ru**

Продам чара (ultima online) на шарде enigma о цене договоримся потом. Мыло **trinsink@mail.ru**



Некоммерческому проекту GTA3: Now In Russia требуются куль программеры, художники и дизигнеры. Свои предложения присылайте на мейл: **dimakro@mail.ru**

Товарищи! Продайте журнал
][акер, за номерами:
01.02(37)
10.01(34)
09.01(33)
07.01(31).
Отмыливать на **elf_ak@mail.ru**





Ищу работу желательно со средним окладом в совершенстве знаю HTML, JavaScripts и Фотошоп. Также немного знаю Флеша и Perl. Создам сайт для кого угодно всего за 300 рублей. Продам диски если нужен прайс лист пишите (диски доставляются по почте с предварительной оплатой). Очень хочу стать хакером ищу наставника! Кого что-то заинтересовало или хочет мне помочь мыльте **dralexxl@mail.ru**





Хороший кодер (Delphi,Assembler) напишет программу (троян,вирус и т.д) на заказ. Заинтересовавшихся прошу мылить на **cyberbono@mail.ru**

Ищу работу. Настройка, сборка, обслуживание ПК. Установка различных программ и программного обеспечения. Подключения к Интернету через протокол TCP\IP. Также достану любую музыку в формате mp3 на заказ. Пишите: **jbanov-anton@mtu-net.ru**

В поисках симпотной, в разговоре, девушки 3-D дисигнер. Буду рад ответить всем! Мыльте на **mccobol@xakep.ru.** Заранее спасибо.



Продам:
Журнал «ХАКЕР» (ver. 06.02(42), без диска) (45р.)
Linux Mandrake 8.0 2CD (1ый - install, 2ой - софт, 90р.) VideoCD «Ужин с придурком» 2CD (100р., новый стоит 150-200р.) Flash 5.0 Rus&Eng (плюс всякие прибамбасы - Dreamweaver, FreeHand и т.д., 50р.) Combat Mission: Beyond Overlord (45р.) Пересылка по почте наложенным платежом.
Мыльте на **banner@mail.ru** и **butt_banner@freemail.ru.**



Каждый чел прекрасно знает комикс/мультфильм «Ghost in the shell». Есть идея создать о нем сервер (материалы имеются). Мой емайл - **pinkerator123@mail.ru**

Если ты знаешь много о компьютерном железе, то давай переписываться.
Мейл: **sergiencou@yandex.ru**

Вступлю в хакерскую, кодерскую или дизайн студию. Знаю HTML, Java, Delphi, Photoshop. Также вступлю в CS клан. Мылить на **head2head@mail.ru**



Продаю легальные аккаунты МТУ. Оплата в системе WebMoney + скидки. Мылить на **sashabox2000@rambler.ru**

Все кто только начинает составлять свои спам-листы давайте обмениваться начинаниями друг с другом! Уже есть лист на 4150 e-mail'ов. Приму любое кол-во адресов начиная от 300 штук и вышлю в ответ столько же и даже больше!
Пишите на **realtemple@mail.ru**

Я собираю прикольные картинки, фразы и выражения, которые можно (нужно) залепить в туалете,на футболке или на будке Тузика... Самое веселое художество ждет награда! Валите все на **lameon@mail.ru**





Куплю старые номера журнала «ХАКЕР»: всё номера за «99 год, Спец-Выпуски по Линуксу, Кодингу. Пересылка наложенным платежом по почте. Пишите на **banner@mail.ru.**

Люди, кто займается разработкой/програмингом исскусственного интелекта, особенно обучающегося: Мыльте, будем общаться: «Тоха» **aimaker@ukr.net**

Буду очень признателен если кто-то расскажет мне как получить бесплатный инет в Питере или по крайней мере хороший тестовый. Отблагодарю ;) **dogger@bk.ru**

Москвичи! Продам старые номера Хакера и его спецвыпусков. **d3m0n@freemail.ru**

Дизайнер и аниматор ищет работу для создание проекта.
Мылить на **expert-work@rambler.ru**



Москва Олди 232 3009, 105 0700; Роско 795 0400; Радом 232 2237; VIST 159 4001; Элси 777 9779; Лизард 490 6536; АЗТ Бизнес-Трейд 742 8355; Белый ветер 730 3030; POLARIS 755 5557; Ф Центр 472 6401; NIX 216 7001, 974 3333; Техмаркет 363 9333; Электроника 158 2641; СтартМастер 935 3852; CITILINK 745 2999; Дилижанс 787 4999; Almer 207 7335; Desten Computers 195 0239; Регард Тур 912 4224; Сетевая Лаборатория 784 6490; Электрон-Сервис 737 4499; **Санкт Петербург** (812) Компьютерная служба 320 8080; АСКоД 325 1555; Компьютерный Мир 303 9047; Компьютер Центр "КЕЙ" 325 3215; КАМЕС 327 8315; IVC 346 8636; CONCOM 320 9080; Мир Техники 393 5566; Алкор 542 5440; Ладога 325 8202; DISPLAY GROUP 273 2263; Альтернатива Синицы 554 3484; Рик 325 3535; Рик 327 3410; **Новосибирск** (3832) Нэта 54 1010; Квеста 33 2407; Аргтон 16 4422; МультиШтерн 53 4444; **Волгоград** (8442) Вист 32 7932; Криста 96 5147; Телетон 72 5550; **Астрахань** (8512) Гранд-Сервис 39 6046; **Мурманск** (8152) ОТС 45 7355; **Ростов на Дону** (8632) Технополис 90 3111; Вист-Дон 63 5430; Микро Системс 63 5777; Зенит 38 65 65; **Краснодар** (8612) Владос 64 2864, 62 2341; Трейд Мастер 55 5040; Компьютерные Системы 55 9994; Окей 60 1144; **Сочи** (8622) Юпитер-Юг 99 8789; Владос 92 2291; **Новороссийск** (27) Владос 22 6442; **Нижний Новгород** (8312) Апрель-Сервис 34 3635; ЭВМ-Спектр 39 0169; Бытовая автоматика 37 1949; Вист 67 7905; Юст 30 1674; **Екатеринбург** (3432) Формоза 59 1868; Техно-групп 77 6552; Класс 59 9821; **Челябинск** (3512) EMS 60 2057; Мединком 60 5762; Форт Электроникс 33 5577; **Оренбург** (3532) Мехатроника 78 0757; **Иркутск** (3952) Алион 51 0510, Комтек 25 8338; **Омск** (3812) Вист 54 4384; Коммед 53 0530; Надежда 31 5658; **Томск** (3822) Intant 56 0056; ЭлексКом 65 7260; **Ижевск** (3412) Элия 43 2026; **Тула** (0872) Вист 30 5100; **Калуга** (0842) Вист-Ока 55 8585; **Рязань** (0912) Комп 24 1070; **Казань** (8432) Абак 76 9559; Марг 64 2584; **Кемерово** (3842) ККЦ 36 0303; **Самара** (8452) Прагма 16 3287; Ламберт 32 6104; Тект-Софт 99 35 75; **Тольятти** (8482) ИнфоЛада 40 6640; Альба 22 9453; **Тюмень** (3452) Комтех 46 6594; **Уфа** (3472) Форте 35 8914; Империал 53 4222; **Ю. Сахалинск** (42422) СахИнфо 33 605; **Хабаровск** (4212) Амур 376587, Конком 32 7580; **Находка** (4236) EPSI 64 6680; **Владивосток** (4232) Информационные Системы 26 9055; Влад-техно 26 8187; **Саранск** (8342) Форго 17 0858; **Ставрополь** (8652) Инфо 77 7777; **Владимир** (0922) Конт 32 6080; **Орел** (0862) Трио 42 5004; **Пенза** (8412) РКЦ 66 4121; **Пермь** (3422) ИВС 19 6500; НПО Индукция 33 1086; **Новокузнецк** (8343) ККЦ 39 0079; **Барнаул** (3852) Алтай Компьютер Сервис 22 3361; Компьютер Трейд 38 1000; **Армавир** (237) Владос 5 9910; **Липецк** (0742) Регард Тур 48 5285

Для получения дополнительной информации www.samsungelectronics.ru